10/758,023
TOMOCHIKA MURAKAMI ET AL
IMAGE PROCESSING METHOD AND IMAGE PROCESSING APPARATUS

CFM 03401
US

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　４月　９日

出願番号
Application Number: 特願２００３－１０５４９８

[ST. 10/C]: [ＪＰ２００３－１０５４９８]

出願人
Applicant(s): キヤノン株式会社

２００４年　１月１４日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３１１１２６９

【書類名】　特許願
【整理番号】　254018
【提出日】　平成15年 4月 9日
【あて先】　特許庁長官殿
【国際特許分類】　G06F　7/00
【発明の名称】　画像処理方法
【請求項の数】　1
【発明者】
【住所又は居所】　東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内
【氏名】　村上　友近
【発明者】
【住所又は居所】　東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内
【氏名】　若尾　聡
【特許出願人】
【識別番号】　000001007
【氏名又は名称】　キヤノン株式会社
【代理人】
【識別番号】　100076428
【弁理士】
【氏名又は名称】　大塚　康徳
【電話番号】　03-5276-3241
【選任した代理人】
【識別番号】　100112508
【弁理士】
【氏名又は名称】　高柳　司郎
【電話番号】　03-5276-3241

【選任した代理人】
　【識別番号】　100115071
　【弁理士】
　【氏名又は名称】　大塚　康弘
　【電話番号】　03-5276-3241
【選任した代理人】
　【識別番号】　100116894
　【弁理士】
　【氏名又は名称】　木村　秀二
　【電話番号】　03-5276-3241
【先の出願に基づく優先権主張】
　【出願番号】　特願2003- 12514
　【出願日】　平成15年 1月21日
【手数料の表示】
　【予納台帳番号】　003458
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　0102485
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　画像処理方法

【特許請求の範囲】

【請求項１】　第１の領域と第２の領域とで構成される原画像に対する改竄の位置を検出可能にするための情報を生成する画像処理方法であって、

前記第１の領域の画像を用いて、前記原画像の特徴画像を生成する特徴画像生成工程と、

前記特徴画像と前記原画像に関する情報とを含む透かし情報を生成する透かし情報生成工程と、

前記透かし情報に対して誤り訂正符号化を行い、誤り訂正符号化透かし情報を生成する誤り訂正符号化工程と、

前記原画像において、前記第２の領域の画像情報を前記誤り訂正符号化透かし情報に置き換えた画像を出力画像として出力する出力工程と

を備えることを特徴とする画像処理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、画像に対して改竄された位置や改竄の有無を検出するための技術に関するものである。

【０００２】

【従来の技術】

近年、従来の銀塩写真や8mmフィルムに変わって、撮影した情報をディジタル化し、ディジタルデータとして記録媒体等に記録するディジタルカメラといった映像入力装置が実用化されている。これにより、撮影した情報そのものをパーソナルコンピュータを始めとする情報処理装置に移し、表示させることが可能になった。また、このような映像データを通信回線を利用することで全国どこでも瞬時に映像データを送信することも可能になった。

【０００３】

そのため、事故処理で証拠写真を扱う保険会社や建築現場の進捗状況の記録を

扱う建設会社においてディジタル映像データの利用が考えられている。しかし一方で目覚しいデータ処理技術の進歩により、映像データを始めとしたディジタルデータの編集をフォトレタッチツールや動画編集ツール等の使用で容易に行うことが可能になった。そのため、ディジタル映像データの信頼性は従来の銀塩写真等と比較して低く、証拠としての能力に乏しいという問題があった。

【０００４】

その為、ディジタルデータに対する原本性を実現する為の技術や改ざん位置を検出する為の技術が数多く開発されてきた。

【０００５】

改ざん検出の技術は一般に大きく分けて二つのアプローチが考えられる。一つはディジタルデータのデータ部分からハッシュ関数を用いて算出したダイジェスト（ハッシュ値）を秘密鍵で暗号化（署名生成）して生成されるディジタル署名をファイルの所定位置（ヘッダ等）に添付するディジタル署名技術である。

【０００６】

もう一方は、一定の規則性を満たす電子透かしをディジタルデータ自体に埋め込み、一定の規則性が満たされているかを検証することでディジタルデータの改ざんの有無や改ざん位置の検出を行う電子透かし技術である。

【０００７】

前者のディジタル署名技術では、画像検証の為のディジタル署名はファイルの所定位置（ヘッダ等）に添付される為、ファイルフォーマット変換によりヘッダの情報が失れた場合、フォーマット変換されたファイルからは改ざん検出ができないというデメリットがある。

【０００８】

一方、後者の電子透かし技術では、一定の規則性を満たす電子透かしをデジタルデータ自体に埋め込む為、ファイルフォーマット変換には耐性があるものの、画質劣化をもたらすという課題がある。

【０００９】

次に、従来の改ざん位置検出用電子透かしについて述べる。従来では、改ざん位置検出用電子透かし埋め込み装置においては、入力画像データを画素毎にふた

つの領域（例えば、８ビットグレースケール画像なら上位７ビットと最下位ビット）に分割し、埋め込み処理対象画素毎に所定の鍵情報から画素位置に依存して生成される乱数と対応する画素位置の一方の画像領域のデータ（例えば上位７ビット）を暗号化関数に入力し、画素毎に透かし情報（１ビット）を生成する。そして生成された透かし情報（１ビット）を対応する分割した他方の画像領域（例えば最下位ビット）のデータと置き換える。この操作を入力画像の全画素に対して行い、改竄位置検出用の電子透かしの埋め込みを行う。

【００１０】

改ざん位置検出装置においては、埋め込み時と同じく、入力画像データを画素毎にふたつの領域に分割し、検証処理対象画素毎に、所定の鍵情報から画素位置に依存して生成される乱数と対応する画素位置の一方の画像領域のデータ（例えば上位７ビット）を暗号化関数に入力し、画素毎に透かし情報（１ビット）を生成する。そして生成された画素毎の透かし情報（１ビット）と対応する分割した他方の画像領域のデータ（例えば最下位ビット）と比較し、ビット値が異なれば改竄、同じであれば改竄が行われていないと見なす。この操作を入力画像の全画素に対して行い、画像中の改ざん位置を検出する。

【００１１】

透かしデータは、画素毎に、画素位置に応じて鍵情報から生成される乱数と一方の画像領域のデータから、暗号化関数を用いて１または０のバイナリーデータとして生成される為、１か０かが反転する場合にのみ改ざんを検出することが出来る。本方式は、アルゴリズムが公開されても良いというメリットがあるものの、所定の鍵情報から生成される乱数が流出すれば、改ざんされていないと見なされる改ざん画像が容易に生成可能な為、この乱数を秘密情報とする必要がある。

【００１２】

また他の従来例では、改ざん位置検出用電子透かし埋め込み装置においては、画像データをふたつの領域に分割し、一方の画像領域から擬似階調画像を生成する。次に擬似階調画像に対し秘密の鍵情報を用いてランダム位置に並べ替えるランダム化処理を行い、埋め込み位置が画像全体に拡散した透かし画像データを生成する。最後に透かし画像を他方の画像領域と置き換え、改ざん位置検出用の透

かしが埋め込まれた画像を出力する。

【００１３】

改ざん位置検出装置では、まず、透かし入りの改ざん画像をふたつの領域に分割し、一方の領域の画像データを取得する。次に、一方の領域の画像データに対し秘密の鍵情報を用いて、埋め込み位置を逆にランダム化し、擬似階調画像を復元する。そして透かし入りの改ざん画像から他方の領域の画像データを取得し、再び擬似階調画像を生成する。

【００１４】

最後に、改ざん画像の一方の領域から復元された擬似階調画像と、他方の領域の画像データから生成された擬似階調画像を比較し、改ざん位置を特定する。

【００１５】

本方式は、アルゴリズムが公開されても良いというメリットがあると共に、復元された擬似階調画像から、元の画像状態が分かるという更なるメリットがある。しかしながら、改ざん時に破損箇所が逆ランダム化により画像全体に散乱する為、正確な改ざん位置が特定できないというデメリットがある。

【００１６】

【発明が解決しようとする課題】

上記後者の従来例による手法では、元の画像状態が分かるというメリットがあるものの、正しい改ざん位置が特定できないという課題があった。

【００１７】

また上記に述べた従来の電子透かし技術を用いた場合、改ざん位置を特定することができるものの、改ざん位置検出用の電子透かしを埋め込む際に必要な鍵情報と改ざん位置検出の際に必要な鍵情報は同一である為、改ざん位置検出の為の鍵情報は、第三者に流出すると容易に改ざんが可能となる為、オープンにすることが出来ず、限定された人物や機器でしか、画像の検証を行うことが出来ない不便さがあった。

【００１８】

本発明は以上の問題に鑑みてなされたものであり、画像に対する改竄の位置を正確に検出することを目的とする。

【００１９】

【課題を解決するための手段】

本発明の目的を達成するために、例えば本発明の画像処理方法は以下の構成を備える。

【００２０】

すなわち、第１の領域と第２の領域とで構成される原画像に対する改竄の位置を検出可能にするための情報を生成する画像処理方法であって、

前記第１の領域の画像を用いて、前記原画像の特徴画像を生成する特徴画像生成工程と、

前記特徴画像と前記原画像に関する情報とを含む透かし情報を生成する透かし情報生成工程と、

前記透かし情報に対して誤り訂正符号化を行い、誤り訂正符号化透かし情報を生成する誤り訂正符号化工程と、

前記原画像において、前記第２の領域の画像情報を前記誤り訂正符号化透かし情報に置き換えた画像を出力画像として出力する出力工程と

を備えることを特徴とする。

【００２１】

【発明の実施の形態】

以下添付図面を参照して、本発明を好適な実施形態に従って詳細に説明する。なお、本発明の手法と従来技術との違いを明確に示す為、はじめに従来技術の説明を行う。

【００２２】

図１５は従来技術であるコンピュータセキュリティシンポジウム２００２で発表された論文「改ざん前の状態が分かるデジタル画像の改ざん検出用電子透かし法」の改ざん位置検出用電子透かし埋め込み装置の機能構成を示すブロック図である。なお、以降の説明では、論文「改ざん前の状態が分かるデジタル画像の改ざん検出用電子透かし法」を論文（１）と呼ぶこととする。

【００２３】

まず、各画素の画素値が８ビットで表現されるグレースケール画像は、領域取

得部１５０１に入力され、ＬＳＢを除く上位７ビットのビットプレーンを画像領域Ａとして、後段の特徴抽出部１５０２に出力する。次に特徴抽出部１５０２では、画像領域Ａに対して、シミュレーティッドアニーリングを用いた方法を用い、２値画像（２次元特徴画像）を後段のランダマイズ部１５０５に出力する。

【００２４】

ここで、代表的な擬似階調画像の作成法の一つに誤差拡散法があるが、誤差拡散法は擬似階調値と原画像の画素値の誤差を順に伝播させながら擬似階調値を計算していく為、改ざん箇所の擬似階調の計算が他の部分の擬似階調の計算に影響を及ぼす。従って改ざん場所の特定が出来なく成る為、特徴抽出部における処理として適さない。前述の論文で用いているシミュレーティッドアニーリング法は原画像と２値画像の視覚的差異をエネルギー関数としてシミュレーティッドアニーリングアルゴリズムによりエネルギーが最小（正確には極小）となる２値画像を求める方法であり、改ざん箇所の擬似階調の計算は、他の部分の擬似階調の計算に影響を与えないというメリットがある。

【００２５】

次に、ランダマイズ部１５０５では、入力された２値画像（２次元特徴画像）に対し、並びをランダム化する処理を行い、並びがランダム化された２値画像（２次元特徴画像）を後段の置換部１５０６に入力する。

【００２６】

最後に置換部１５０６では、入力画像のＬＳＢのビットプレーンを、ランダマイズ部から入力されるランダム化された２値画像に置き換え、透かし入り画像を生成する。

【００２７】

図１６は論文（１）における改ざん位置検出装置の機能構成を示すブロック図である。

【００２８】

まず、改ざんが施された改ざん画像は分離部１６０１に入力される。分離部１６０１では、入力画像を画像領域Ａ（ＬＳＢを除く上位７ビットのビットプレーン）と画像領域Ｂ（ＬＳＢのビットプレーン）に分離し、それぞれ後段の特徴抽

出部１６０５と逆ランダマイズ部１６０２に出力する。

【００２９】

次に逆ランダマイズ部１６０２では、分離部１６０１から入力された画像領域Ｂ、すなわち２値画像（ＬＳＢのビットプレーン）に対し、改ざん位置検出用電子透かし埋め込み装置におけるランダマイズ部１５０５と逆のランダム化処理を行い、原画像の特徴を表す一部が破壊された２値画像を後段の比較部１６０６に出力する。このとき論文（１）では、改竄が検出不能な改ざん画像を生成させない為に逆ランダマイズ部１６０２における並び換えのための情報を秘密の鍵情報として保つ必要がある。

【００３０】

次に特徴抽出部１６０５では、入力された画像領域Ａ（ＬＳＢを除く上位７ビットのビットプレーン）に対し、改ざん位置検出用電子透かし埋め込み装置における特徴抽出部１５０２と同様の処理を行い、改ざん画像の特徴が抽出された２値画像を生成し、後段の比較部１６０６に出力する。

【００３１】

比較部１６０６では、逆ランダマイズ部１６０２から入力される原画像の特徴を表す一部が破壊された２値画像と特徴抽出部１６０５から入力される改ざん画像の特徴が抽出された２値画像とを比較し、改ざん位置を特定する。しかし、論文（１）では既に簡単に述べたが、以下に述べるような改ざん位置を誤る課題がある。

【００３２】

論文（１）では、改ざん位置検出装置において、逆ランダマイズ部１６０２に入力される改ざん画像の画像領域Ｂは、改ざん操作によって一部が破壊される可能性が高い。一部が破壊された画像領域Ｂは、ランダム化処理により、破壊された部分を画像全体に拡散するため、誤りが画像全体に散乱された２値画像を得ることが出来る。しかし、比較部１６０６で画像領域Ａから算出される２値画像（２次元特徴画像）と比較する時、誤りが画像全体に散乱している為、正確な改ざん位置を特定することが出来ず、実際には改ざんされていない画像位置に対して改ざんを検出する可能性がある。

【００３３】

次に、本発明に係る画像処理装置を改竄位置検出用電子透かし埋め込み装置、改竄位置検出装置に適用した実施形態について説明する。

【００３４】

［第１の実施形態］

＜改ざん位置検出用電子透かし埋め込み装置＞

はじめに、公開鍵、即ち誰でも入手可能な鍵で改竄位置検出が可能な電子透かしの埋め込みを行う電子透かし埋め込み装置について説明する。

【００３５】

図１は改ざん位置検出用電子透かし埋め込み装置の機能構成を示すブロック図である。同図に示した各部はハードウェアにより構成されていても良いし、各部の機能をプログラムにより表現し、コンピュータに読み込ませて実現させても良い。

【００３６】

図２は、１画素が８ビットから成る入力画像をビットプレーン毎に示した図である。説明を分かりやすくするため、本実施形態では、入力画像は図２に示すような１画素８ビットからなるグレースケール画像であるとする。

【００３７】

以下、図１を参照して、改竄位置検出用電子透かし埋め込み装置が行う処理について説明する。

【００３８】

まず、入力画像（以下、原画像と呼称する場合もあり、例えば縦５１２画素×横５１２画素とする）は、領域取得部１０１に入力される。領域取得部１０１では、入力画像から所定の画像領域Ａを取得し、後段の特徴抽出部１０２に入力する。説明を分かりやすくするため、領域取得部１０１では、入力画像の最下位（ＬＳＢ）のビットプレーン（図２に示したビットプレーン２０２）を除く上位７ビットのビットプレーン（図２に示したビットプレーン群２０１）を画像領域Ａとして取得するとする。

【００３９】

次に、特徴抽出部１０２では、入力された画像領域Ａの画像、即ち入力画像の上位７ビットのビットプレーンで表現される画像を用いて入力画像の特徴を表現した２次元特徴画像を出力する。

【００４０】

図３は入力画像、２次元特徴画像、そして後述するランダム化された誤り訂正符号化暗号化透かし情報によって表現される画像を示す図である。

【００４１】

特徴抽出部１０２から出力される２次元特徴画像は、同図に３０２で示すように、入力画像３０１よりも縦横の大きさが小さな１ビットの画像となる。詳しくは後述するが、これは、２次元特徴画像を暗号化、誤り訂正符号化した後でも画像領域Ｂ（本実施形態では入力画像のＬＳＢ）に収まるようにするためである。

【００４２】

特徴抽出部１０２で行われる処理の一例としては、画像領域Ａに値が全てゼロのＬＳＢを追加することで、各画素の画素値が８ビットで表現される画像を生成し、更にこの画像の縦横のサイズを半分に縮小し、縮小した画像の各画素値を所定のマトリクス（例えばベイヤーマトリクスなど）の値と比較することで２値化する（組織的ディザ処理）といった処理が考えられる。またディザ処理ながら高品位な２値画像が得られるブルーノイズマスク法なども存在する。その他には輪郭抽出処理もあげられる。また論文（１）で述べられるシミュレーティッドアニーリング法を特徴抽出部１０２で用いてもよい。

【００４３】

入力画像が文書画像の場合にはレイアウト解析及びOCR処理を施し、文字情報や２次元レイアウトを格納可能な文章フォーマットに、OCRで抽出した文字やレイアウト情報を格納し、２次元特徴画像としてもよい。以上のように、特徴抽出部１０２において行われる処理は様々な種類が設計可能である。

【００４４】

特徴抽出部１０２において行われる好ましい処理は、入力画像全体の特徴を抽出できることと、一部を局所的に変化させた入力画像から作成される２次元特徴画像は、局所的に変化させた箇所以外は元と変わらない２次元特徴画像を作成で

きることである。

【００４５】

図３の３０１は入力画像のイメージ図であり、３０２は２次元特徴画像のイメージ図である。本実施形態では２次元特徴画像を生成するために、入力画像に対する縦横のサイズを半分に縮小し、２値化処理するが、縮小処理や２値化処理は必ずしも必須の処理ではなく、画像領域Ｂに２次元特徴画像を納める十分なサイズがあれば、等倍の大きさの２次元特徴画像を生成してもよいし、多値階調の２次元特徴画像を生成してもよい。

【００４６】

次に、２次元特徴画像を暗号化部１０３に入力する。暗号化部１０３ではまず、入力される２次元特徴画像と種々のデータを必要に応じて組み合わせ、改ざん位置検出用透かし情報を生成する。以降、「透かし情報」あるいはｗは改ざん位置検出用透かし情報を表すとする。

【００４７】

図８は「透かし情報」の概略構成を示す図である。同図には８０１～８０４の複数の「透かし情報」の構成例を示しているが、「透かし情報」の内部構成は８０１～８０４の構成例に限定されないものとする。

【００４８】

２次元特徴画像と組み合わせる種々のデータとしては、図８の８０１に示すような正しい復号化が行われたかチェックする目的の「検査ビット」や８０２に示すような２次元特徴画像の縦と横の長さを２進数で表す「縦長」、「横長」、２次元特徴画像を生成する際に用いた特徴抽出処理を特定する情報の１つである「特徴抽出処理ＩＤ」などがあげられる。さらに図示しないが、「２次元特徴画像のビット長」や「撮影日時」やＧＰＳから得られる「位置情報」や「撮影デバイスのシリアル番号」、「撮影者情報」などを追加してもよい。

【００４９】

検査ビットは少なくとも２次元特徴画像を含む透かし情報の一部（２次元特徴画像や「縦長」、「横長」、「特徴抽出処理ＩＤ」等の情報）の整合性を検証する為のビット情報であり、例としては、少なくとも２次元特徴画像を含む透かし

情報の一部をハッシュ関数に入力して得られるハッシュ値が挙げられる。ハッシュ関数は、入力値が僅かな変化に対しても、大きく異なる固定長の値を返す性質がある。従って、ハッシュ値を用いた検査ビットを用いれば、僅かな変化に対しても高い精度で整合性の検証が行うことが可能である。また検査ビットとして２次元特徴画像に誤りが無いかを調べるチェックサム（検査合計）を用いることも可能である。

【００５０】

次に暗号化部１０３では、生成された透かし情報に対して、暗号化処理を施す。暗号化部１０３では、様々な暗号方式が利用可能であるが、公開鍵暗号方式を用いる場合、秘密鍵を所有する人物や機器でなくとも、対応する公開鍵で改ざん位置検出が可能になるという大きなメリットを実現できる。その為、本実施形態では公開鍵暗号方式に従って暗号化処理を行うものとする。しかし、暗号化部１０３で共通鍵暗号方式を用いることも可能である。このとき、改ざん位置の検出は共通鍵を持った人物や機器でしか行えないデメリットがあるが、共通鍵暗号方式を用いる場合、公開鍵暗号方式に比べ高速に処理できるメリットもある。

【００５１】

既に周知の技術であるので詳しい説明は省くが、公開鍵暗号方式では、秘密鍵を用いて暗号化されたデータは公開鍵で容易に復号可能であるが、秘密鍵を知らない限り公開鍵で復号できる正しく整合性の取れたデータを生成することは実質不可能である。

【００５２】

従って、秘密鍵がデジタルカメラやデジタルビデオカメラなどの撮像デバイス内部で読み出されないように厳重に管理されているなら、秘密鍵に対応する公開鍵で復号可能な改ざん後の画像データと対応する２次元特徴画像を含む暗号化した透かし情報を生成することは実質不可能である。なお、公開鍵暗号方式としては、RSA暗号や楕円暗号などがよく知られている。

【００５３】

暗号化部１０３では透かし情報に対し公開鍵暗号方式を用いて秘密鍵で暗号化（署名生成）を行い、暗号化透かし情報を出力する。以降、Ｃ（ｗ）は暗号化透

かし情報を表すとする。

【００５４】

ここで暗号化透かし情報Ｃ（ｗ）の情報量について考える。暗号化部１０３から出力される暗号化透かし情報Ｃ（ｗ）は、入力データである透かし情報ｗと比べてデータの大きさが変化する可能性がある。例えば、暗号化部でRSA暗号を用いた場合、透かし情報ｗは鍵長の単位で処理される為、Ｃ（ｗ）は鍵長に比例した長さとなる。

【００５５】

今、暗号化部１０３で用いるRSA暗号の鍵長を１０２４ビットとし、暗号化部１０３に入力される２次元特徴画像は各画素１ビットの縦２５６画素、横２５６画素（６５５３６ビット）であり、検査ビットが２次元特徴画像から計算される１６０ビットのハッシュ値であるとすると、暗号化部１０３に入力される透かし情報は６５６９６ビットとなる。既に述べたように、ＲＳＡ暗号では、鍵長の単位で入力データを処理する為、最後の１０２４ビットに満たないビット情報（１６０ビット）に対しては所定のビット値（例えばゼロ）が付加（パディング）されて１０２４ビット単位で処理される。従って、暗号化部１０３から出力される暗号化透かし情報Ｃ（ｗ）のビット長は鍵長の整数倍となり、６６５６０ビットとなる。

【００５６】

このように、暗号化処理時に透かし情報の末尾に所定のビット（例えばゼロ）が付加される場合、復号時の透かし情報でも透かし情報の末尾に所定のビット（例えばゼロ）が付加されている。予め２次元特徴画像のサイズが分からないときには、透かし情報に含められる情報である「縦長」「横長」（透かし情報の構成が図８中の８０２や８０４に示す構成である場合）を利用し、２次元特徴画像データの長さを計算することで、透かし情報中に含められている２次元特徴画像を正しく抽出できる。

【００５７】

また、透かし情報は暗号化処理を行う前に鍵長の整数倍にパディング処理されてから暗号化処理を施されるが、その際にパディングするビットを予め決められ

た固定のビットとすることで、パディングするビットに「検査ビット」と同様の役割を兼ねさせることも可能である。

【００５８】

次に、暗号化透かし情報Ｃ（ｗ）は、誤り訂正符号化部１０４に入力される。誤り訂正符号化部１０４では入力された暗号化透かし情報Ｃ（ｗ）に対し、誤り訂正符号化処理を行い、誤り訂正符号化暗号化透かし情報を出力する。以降、ＥＣＣ（Ｃ（ｗ））は誤り訂正符号化暗号化透かし情報を表すとする。

【００５９】

誤り訂正符号化部１０４で用いる誤り訂正符号としては、ＢＣＨ符号、リードソロモン符号、畳み込み符号、ターボ符号など様々な符号が存在するが、予想される改ざん、即ち発生する誤りの種類により、適切な誤り訂正符号を用いるとよい。

【００６０】

一般に誤りの種類として、ビット毎に独立に発生する「ランダム誤り」や部分的に集中して連続的に発生する誤り「バースト誤り」や、所定のビットからなる小ブロック（バイトと呼ぶ）毎に発生する「バイト誤り」などがある。「ランダム誤り」には「ＢＣＨ符号」、「バイト誤り」には「リードソロモン符号」が有効であるといわれている。なお、「リードソロモン符号」で符号化した後にインターリーブ処理（例えばランダム化処理）を加えることで、「バースト誤り」に強くすることが可能である。なお、インターリーブ処理としてはランダム化処理に限らず、情報系列の並びを攪拌する為の種々の方式や設計が存在する。本実施形態ではインターリーブ処理としてランダム化処理を例に説明を行うが、インターリーブ処理は情報系列の並びを攪拌する処理とし、ランダム化処理に限らないとする。

【００６１】

画像の改ざんとしては、一般に画像の特定の箇所に集中した改ざんが想定される。従って画像に対して「バースト誤り」に強い符号を用いた誤り訂正符号化を行うことで、特定の箇所に集中した改ざんを「バースト誤り」として検出することができる。

【００６２】

しかし「バースト誤り」に強い符号を用いずとも、暗号化透かし情報Ｃ（ｗ）を符号化後にインターリーバでランダム化処理を施すことで、「バースト誤り」に強くすることも可能である。なお、このとき誤り訂正符号を復号側では、誤り訂正符号化暗号化透かし情報ＥＣＣ（Ｃ（ｗ））に対して誤り訂正復号処理を行う前にデインターリーバで逆ランダム化処理を施し、符号化ビット列の順序を元に戻してから復号する必要がある。

【００６３】

図６はそれぞれ透かし情報（６０１）、暗号化透かし情報（６０２）、誤り訂正符号化透かし情報（６０３）、ランダム化誤り訂正符号化透かし情報（６０４）のビット長を比較、説明するための概略図である。

【００６４】

誤り訂正符号化暗号化透かし情報６０３は、冗長なビットが誤り訂正の目的で加算される為、暗号化透かし情報６０２と比べ、情報量（同図ではビット長に反映されている）が増加している。

【００６５】

誤り訂正符号化部１０３における誤り訂正符号化のパラメータは、暗号化透かし情報ＥＣＣ（Ｃ（ｗ））の情報量が画像領域Ｂ（第１の実施形態ではＬＳＢのビットプレーン）に正確に収まる情報量になるように設計するとよい。例えば、誤り訂正符号のパラメータを固定にして、暗号化された透かし情報量にパディング処理を施して、誤り訂正後に画像領域Ｂに正確に収まる情報量にしてもよいし、パディング処理ではなくチェックサムなどを加え、より正確に誤り訂正復号を行えるようにしてもよい。また、誤り訂正符号のパラメータをパディングやチェックサムなしに、誤り訂正符号化後に画像領域Ｂに正確に収まる情報量になるように誤り訂正符号部１０３のおけるパラメータを設定しても良い。

【００６６】

図７は誤り訂正符号化を行う前の透かし情報Ｃ（ｗ）の一例を示す図である。図７では、誤り訂正符号化後に画像領域Ｂに正確に収まるように、末尾に所定のビット（例えば０）をパディングしてあるが、このとき、誤り訂正符号化を行う

前の暗号化透かし情報Ｃ（ｗ）に、暗号化透かし情報のビット長を記すビット列を「暗号化透かし情報のビット長」の位置に２進数で記録すれば、仮にパディングが存在したとしても、暗号化された透かし情報の部分のビット列を正しく抽出することも出来る。

【００６７】

誤り訂正符号化１０４では、暗号化透かし情報Ｃ（ｗ）のサイズが小さいほど（即ち、２次元特徴画像の情報が少ないほど）誤り訂正符号化部１０４で冗長性を生かし誤り訂正の能力を強力にすることが出来る。

【００６８】

その結果、透かしが埋め込まれた画像に対して大きな改ざんが施された場合でも、改ざん位置の特定が可能となる。逆に２次元特徴画像の情報が多いほど、誤り訂正符号化部１０４で強い誤り訂正を行うことが出来なくなる。

【００６９】

２次元特徴画像の情報量と誤り訂正符号の強さ（改ざんに対する強さ）はトレードオフの関係にあるので、本実施形態によれば、用途に応じて２次元特徴画像の情報量と誤り訂正符号の強度パラメータを決定することが出来る。このように用途に応じてパラメータを柔軟に設定できる点は、本実施形態の大きな長所の一つである。２次元特徴画像の情報量と誤り訂正符号の強度パラメータは、経験的に得られるデフォルトパラメータで設定してもよいし、撮像デバイスで撮影画像に応じて自動的に決定してもよいし、また改ざん位置検出用電子透かしの埋め込み時にユーザに選択させても良い。

【００７０】

次に、誤り訂正符号化暗号化透かし情報ＥＣＣ（Ｃ（ｗ））は、インターリーバ１０５に入力される。インターリーバ１０５では、入力された誤り訂正符号化暗号化透かし情報ＥＣＣ（Ｃ（ｗ））を構成するビット列をランダムに並べ替える操作を行い、ランダム化された誤り訂正符号化暗号化透かし情報を出力する。このとき並べ替えに用いる鍵情報は改ざん位置検出時にも必要となるが、本実施形態においてはこの鍵情報を用いても改ざんが不可能であるため、公開情報としてよい。

【００７１】

なお、インターリーバ１０５は必ずしも必須のブロックではなく、誤り訂正符号化部１０４で特定の箇所に集中した改ざん（バースト誤り）に対しても誤り訂正能力がある誤り訂正符号を用いる場合やターボ符号のように誤り訂正符号内部にインターリーバの機能を有している誤り訂正符号を用いる場合には不要である。

【００７２】

以降、Ｓ（ＥＣＣ（Ｃ（ｗ））はランダム化された誤り訂正符号化暗号化透かし情報を表すとする。

【００７３】

最後に、インターリーバ１０５でランダム化された誤り訂正符号化暗号化透かし情報Ｓ（ＥＣＣ（Ｃ（ｗ））は、置換部１０６に入力され、入力画像の所定の画像領域Ｂ（本実施形態では図２の２０２に相当するＬＳＢのビットプレーン）と置き換えが行われ、ランダム化された誤り訂正符号化暗号化透かし情報Ｓ（ＥＣＣ（Ｃ（ｗ））が埋め込まれた透かし入り画像を出力画像として出力する。

【００７４】

図３の３０３は、置換部１０６でＬＳＢのビットプレーンと置き換えられるランダム化された誤り訂正符号化暗号化透かし情報Ｓ（ＥＣＣ（Ｃ（ｗ））をラスター順に並べ、画像として表現した場合のイメージ図である。暗号化処理や誤り訂正符号化処理により、情報量が２次元特徴画像３０２に比べて増大している。

【００７５】

例えば、入力画像を縦５１２画素×横５１２画素の各画素８ビットのグレースケール画像とし、２次元特徴画像は縦２５６画素×横２５６画素の各画素１ビットのモノクロ画像とし、誤り訂正符号化暗号化透かし情報Ｓ（ＥＣＣ（Ｃ（ｗ））は縦５１２画素×横５１２画素の各画素１ビットのモノクロ画像とすると理解しやすい。

【００７６】

＜改ざん位置検出装置＞

次に改ざん位置検出装置について詳しく説明する。図４は改ざん位置検出装置の機能構成を示すブロック図である。同図に示した各部はハードウェアにより構成されていても良いし、各部の機能をプログラムにより表現し、コンピュータに読み込ませて実現させても良い。

【００７７】

図５は、改ざんが行われた改ざん画像から改ざん位置を判定する処理を説明するための図である。以下、図４のブロック図に従って、図５を用いながら、改ざん位置検出装置が行う処理を説明する。

【００７８】

図５において５０１は改竄がなされた画像を示し、５１０の領域（網掛けされた三日月の形状の領域）が改竄がなされた領域を示す。以下の説明では５０１に示す改竄画像を例に取り説明するが、各種の改竄画像に対しても以下説明する処理は適用可能である。

【００７９】

改ざん画像５０１（入力画像）は、改ざん位置の検証の為、分離部４０１に入力される。分離部４０１では入力画像を画像領域Ａと改ざん位置検出用の透かし情報が埋め込まれている画像領域Ｂに分離する。本実施形態では、埋め込み装置と同じく、図２に示すように画像領域Ａは最下位（ＬＳＢ）のビットプレーンを除く上位７ビットのビットプレーン２０１とし、画像領域ＢはＬＳＢのビットプレーン２０２とする。

【００８０】

図５において５０２は、入力画像から得られる画像領域Ｂを示す画像データである。入力画像から得られる画像領域Ｂの画像データは５０２に示すように、改ざん位置（５２０で示す領域の位置）で破壊されている可能性がある。

【００８１】

次に、分離部４０１で分離された画像領域Ｂのデータは、デインターリーバ４０２に入力される。デインターリーバ４０２では、一部が壊れたランダム化された誤り訂正符号化暗号化透かし情報Ｓ’（ＥＣＣ（Ｃ（ｗ））を構成する各ビ

ット列の並びを、元のビットの並びに戻す処理を行う。

【００８２】

デインターリーバ４０２はランダム化を解除した一部が壊れた誤り訂正符号化暗号化透かし情報（以降、ＥＣＣ’（Ｃ（ｗ））と表現する）を後段の誤り訂正復号化部４０３に出力する。なお、誤り訂正符号の種類によっては、埋め込み時にインターリーバを必要としない場合がある。従って、デインターリーバ４０２における処理は必須ではなく、埋め込み時にインターリーバ１０５でＥＣＣ（Ｃ（ｗ））をランダム化した場合にのみ必要となる。

【００８３】

次に、デインターリーバ４０２から出力されるＥＣＣ’（Ｃ（ｗ））は、誤り訂正復号部４０３に入力される。誤り訂正復号部４０３では入力された一部が破壊されたＥＣＣ’（Ｃ（ｗ））に対して誤り訂正復号を行い、暗号化された透かし情報Ｃ（ｗ）を後段の暗号復号部４０４に出力する。

【００８４】

ここで、画像領域Ｂの透かしデータが改ざんにより大きく破壊され、誤り訂正符号が正しく誤り訂正復号が出来ない場合（但し、誤り訂正符号自体に正しく誤り訂正復号できないことを伝える機能を持っている必要がある）、「改ざん位置の特定はできないが、画像全体が改ざんされている」旨を結果として表示し、処理を終了する。

【００８５】

次に暗号復号部４０４に入力された誤り訂正復号された暗号化透かし情報Ｃ（ｗ）は、公開鍵暗号方式で、暗号化に用いた秘密鍵に対応する公開鍵を入手し、公開鍵を用いて、暗号化透かし情報Ｃ（ｗ）を復号化し、透かし情報ｗを復元する。

【００８６】

改ざん位置検出に用いる公開鍵が正しいとき、暗号復号部４０４では、透かし情報ｗを構成する検査ビットの値をチェック（検査ビットが２次元特徴画像のハッシュ値である場合は、透かし情報ｗに含まれる２次元特徴画像からハッシュ値を計算し、透かし情報ｗ中の検査ビットと一致するか否かを比較）することで、

正しい秘密鍵で暗号化（署名生成）された暗号化透かし情報Ｃ（ｗ）であるか、異なる秘密鍵で暗号化（署名生成）された暗号化透かし情報Ｃ（ｗ）であるかを識別することが出来る。公開鍵暗号方式では、秘密鍵の知識がなければ、公開鍵で復号できる正しく整合性の取れた透かし情報を生成することは出来ない。

【００８７】

従って、検査ビットの値が一致しないならば、暗号化透かし情報Ｃ（ｗ）は正しい秘密鍵で暗号化されていないことを意味する。そこでこのような場合は、「不正な改ざんが行われている」旨をユーザに通知し、処理を終了する。なお、改ざん位置検出に用いる公開鍵を誤って用いた場合にも検査ビットの値は誤るので、「復号に用いる鍵が異なる」旨をユーザに通知してもよい。

【００８８】

暗号復号部４０４では図６の６０１に相当する、暗号化が解除された透かし情報ｗの中から２次元特徴画像を取り出し、後段の比較部４０６に出力する。図５の５０４は、改ざん画像の画像領域Ｂ５０２から復元された２次元特徴画像を示す。図５の５０４に示すように、透かし情報ｗの中から取り出された２次元特徴画像は、上記原画像に対する相似画像である。

【００８９】

なお、暗号復号部４０４で復号された透かし情報に「特徴抽出処理ＩＤ」が含まれている場合には、特徴抽出処理ＩＤに基づき、特徴抽出部４０５で行う特徴抽出処理の種別を決定するなどしてもよい。

【００９０】

次に特徴抽出部４０５では、分離部４０１から入力される画像領域Ａに対し、特徴抽出処理を行う。このとき、特徴抽出処理は透かし埋め込み時に生成した２次元特徴画像の生成方法と同じ処理である。そして、特徴抽出部４０５は特徴抽出処理によって得られる２次元特徴画像を後段の比較部４０６に出力する。

【００９１】

図５の５０３は改ざん画像から上記特徴抽出処理によって得られる２次元特徴画像を示す。このとき図５の５０３に示すように、改ざん画像から計算された２次元特徴画像は、改ざんを反映した２次元特徴画像となることが想定される（同

図に示した例では、入力画像５０１における改竄領域５１０が反映されている改竄領域５３０として反映されている）。

【００９２】

最後に比較部４０６では、暗号復号部４０４から入力される正しく復元された２次元特徴画像と特徴抽出部４０５から入力される改ざん情報が反映された２次元特徴情報を比較し、２つの２次元特徴画像の間で値が異なる箇所（即ち、改竄の位置）を画像の検証者に示す。図５の５０５は２次元特徴画像５０３と２次元特徴画像５０４の差分を表す画像（２次元特徴画像５０３と２次元特徴画像５０４とで対応する画素の画素値の差分の集合による画像）である。比較部４０６は例えば、差分画像５０５を生成し、表示部にこの差分画像５０５を表示させることで、改ざん位置を画像の検証者に視覚的に示すことが出来る。

【００９３】

また、改ざん画像から計算された２次元特徴画像５０３と画像領域Ｂから復元された２次元特徴画像５０４を一覧表示させることで、差分画像５０５のように改ざん位置を視覚的に検証者に対して提示するだけではなく、２次元特徴画像上でどの位置が原画像と比べて変化したかという改ざんの内容を画像の検証者に視覚的に明確に示すことが可能になる。

【００９４】

図５の５０６は、差分画像５０５を改ざん画像５０１の大きさに拡大し、改ざん画像５０１上に重ね合わせて（オーバーレイして）表示した画像である。このようにすることで、視覚的に改ざん位置を分かり易く表示することも可能である。このとき、２次元特徴画像の縦横の大きさが入力画像よりも小さい場合、画像５０６のように、改ざん位置は厳密に１画素単位で特定出来ないが、大きな改ざんの場合、実用上十分効果がある。

【００９５】

従来技術である論文（１）で述べられた手法と第１の実施形態に係る手法とを対比して考えると、従来技術においてランダマイズ部１５０５は本実施形態におけるインターリーバ１０５に相当する機能を実行していることが分かる。また、本実施形態の改ざん位置検出用電子透かし埋め込み装置に存在する暗号化部１０

３および誤り訂正符号化部１０４に相当する機能は、従来技術の論文（１）では存在しないことが分かる。

【００９６】

また、改ざん位置検出装置でも同様に、従来技術において逆ランダマイズ部１６０２は本実施形態におけるデインターリーバ４０２に相当する機能を実行していることが分かる。また、本実施形態の改ざん位置検出用電子透かし埋め込み装置に存在する誤り訂正復号化部４０３、暗号復号部４０４に相当する機能は、従来技術の論文（１）では存在しないことが分かる。

【００９７】

本実施形態では誤り訂正符号を導入することで従来技術の論文（１）と比べて、改ざん位置をより正確に特定し、更に公開鍵暗号化を導入することで安全性と利便性の高い改ざん位置検出システムを実現していることが分かる。

【００９８】

以上、本実施形態では、“アルゴリズム公開”かつ“秘密情報を用いずに画像の改ざん位置判定が可能”である改ざん位置検出用透かし埋め込み方法および改ざん位置検出方法について詳しく述べた。

【００９９】

なお、本実施形態は、改ざん前と改ざん後の画像から同じ２次元特徴画像が生成されるような僅かの改ざんの場合、改ざんの有無を検出することが出来ない。しかし、僅かな変更を改ざんと見なさないロバスト性を実現した僅かな変化に対してロバストな画像検証方法であると言える。これは従来の論文（１）においても実現できなかった技術である。

【０１００】

画像に影響のない僅かな変化に対して改ざんの有無の検出する必要がある場合は、追加の手段、例えば、画像データ全体をハッシュ関数に入力し、ダイジェスト（ハッシュ値）を計算し、そのダイジェスト（ハッシュ値）を秘密鍵で暗号化（署名生成）し、画像ファイルのヘッダなどの所定位置にディジタル署名として添付する方法でも実現可能である。

【０１０１】

［第２の実施形態］

＜改ざん位置検出用電子透かし埋め込み装置＞

本実施形態に係る埋め込み装置は、第１の実施形態に係る埋め込み装置によって生成される透かし情報に、画像領域Ａを用いて計算されるダイジェスト（ハッシュ値）を更に加える処理を行う。これにより、画像の改ざん位置だけでなく、画像の改ざんの有無も判定可能にする。

【０１０２】

図９は本実施形態に係る改ざん位置検出用電子透かし埋め込み装置の機能構成を示すブロック図である。なお同図において、図１に示したものと同じものについては同じ番号を付けており、その説明を省略する。また、同図に示した各部はハードウェアにより構成されていても良いし、各部の機能をプログラムにより表現し、コンピュータに読み込ませて実現させても良い。

【０１０３】

図９において図１と大きく異なる点は新たにハッシュ算出部９０７が追加された点である。また、暗号化部９０３は、暗号化部１０３が行う処理と同様の処理を行って第１の実施形態で説明した透かし情報を生成し、この透かし情報に更にハッシュ算出部９０７が生成したハッシュ値のデータを含める処理を行う。

【０１０４】

以下、図９を用いて本実施形態における改ざん位置検出用電子透かし埋め込み装置を説明する。なお第１の実施形態と同様の処理を行うブロックについては説明を簡素化する。

【０１０５】

まず、第１の実施形態と同じく入力画像は、領域取得部１０１に入力される。領域取得部では、入力画像から所定の画像領域Ａを取得し、後段の特徴抽出部１０２および後段のハッシュ算出部９０７に入力する。本実施形態でも説明を分かりやすくするため、画像領域Ａは最下位（ＬＳＢ）のビットプレーンを除く上位７ビットのビットプレーンとする。

【０１０６】

次に特徴抽出部１０２では、入力された画像領域Ａ、即ち上位７ビットのビッ

トプレーンを用いて入力画像の特徴を抽出し、２次元特徴画像を出力する。

【０１０７】

次に、ハッシュ算出部９０７では、画像領域Ａの画像データをハッシュ関数に入力し、ダイジェストを生成し、後段の暗号化部９０３に入力する。

【０１０８】

ここでハッシュ関数について簡単に説明を行う。ハッシュ関数とは可変長データを入力とし、固定長のデータ（ダイジェスト又はハッシュ値と呼ぶ）を計算して出力する関数であるが、主に以下のような特徴を持つ。

【０１０９】

（１）　入力データ長が異なっても、固定長のダイジェストを出力

（２）　入力データが僅かに異なれば、出力ダイジェストは大きく異なる

（３）　ダイジェストから元の入力データを生成できない

（４）　同じダイジェストを出力する入力データを検出することは困難

現在、代表的なハッシュ関数としては、ＭＤ２、ＭＤ４、ＭＤ５、ＳＨＡ－１などがある。ＳＨＡ－１の場合、出力ダイジェストのサイズは１６０ビット（２０バイト）である。上記のようなハッシュ関数においては、画像領域Ａの一部を改ざんした場合に、同じダイジェストを得られる確率は非常に低く、ダイジェストを用いれば画像の僅かな改ざんでも容易に検出できる。

【０１１０】

次に、暗号化部９０３では、特徴抽出部１０２から入力される２次元特徴画像及びハッシュ算出部９０７から入力されるダイジェスト、検査ビットなどを組み合わせ、図８の８０３に示すような、改ざん位置検出用透かし情報を生成する。なお、必要に応じて、第１の実施形態で述べたような「横長」「縦長」「特徴抽出処理ＩＤ」などを記録するビット領域を設けてもよい。

【０１１１】

次に暗号化部９０３では、生成された透かし情報に対して暗号化処理を施す。暗号化部９０３では第１の実施形態と同じく公開鍵暗号方式を用い、透かし情報に秘密鍵で暗号化（署名生成）を行い、暗号化透かし情報Ｃ（ｗ）を出力する。

【０１１２】

次に、暗号化透かし情報Ｃ（ｗ）は、誤り訂正符号化部１０４に入力される。誤り訂正符号化部１０４では入力された暗号化透かし情報Ｃ（ｗ）に対し、誤り訂正符号化処理を行い、誤り訂正符号化暗号化透かし情報ＥＣＣ（Ｃ（ｗ））を出力する。

【０１１３】

次に誤り訂正符号化暗号化透かし情報ＥＣＣ（Ｃ（ｗ））は、インターリーバ１０５に入力される。インターリーバ１０５では入力された誤り訂正符号化暗号化透かし情報ＥＣＣ（Ｃ（ｗ））に対し、ビット列をランダムに並べ替える操作を行い、ランダム化された誤り訂正符号化暗号化透かし情報Ｓ（ＥＣＣ（Ｃ（ｗ））））を後段の置換部１０６に出力する。なお、第１の実施形態と同じく、インターリーバ１０５は必ずしも必須のブロックではなく、誤り訂正符号化部１０４で特定の箇所に集中した改ざんに対しても誤り訂正能力がある誤り訂正符号を用いる場合やターボ符号のように誤り訂正符号内部にインターリーバの機能を有している誤り訂正符号を用いている場合には不要である。

【０１１４】

最後に、インターリーバ１０５でランダム化された誤り訂正符号化暗号化透かし情報Ｓ（ＥＣＣ（Ｃ（ｗ））は、置換部１０６に入力され、入力画像の所定の画像領域Ｂ（本実施形態では図２の２０２に相当するＬＳＢのビットプレーン）と置き換えが行われ、ランダム化された誤り訂正符号化暗号化透かし情報Ｓ（ＥＣＣ（Ｃ（ｗ））が埋め込まれた透かし入り画像を出力画像として出力する。

【０１１５】

＜改ざん位置検出装置＞

次に本実施形態に係る改ざん位置検出装置について説明する。図１０は本実施形態に係る改ざん位置検出装置の機能構成を示すブロック図である。なお同図において、図４に示したものと同じものについては同じ番号を付けており、その説明を省略する。また、同図に示した各部はハードウェアにより構成されていても良いし、各部の機能をプログラムにより表現し、コンピュータに読み込ませて実現させても良い。

【０１１６】

図１０において図４と大きく異なる点は新たにハッシュ算出部１００７が追加された点である。また、比較部１００６は第１の実施形態に係る比較部４０６が行う処理に加えて、ダイジェストを用いた改竄の有無を通知する処理も行う。以下、図１０を用いて本実施形態に係る改ざん位置検出装置について説明する。なお第１の実施形態と同様の処理を行うブロックについては説明を簡素化する。

【０１１７】

まず、図５の５０１に示されるような改ざんが施された画像は、分離部４０１に入力される。分離部４０１では入力画像を画像領域Ａと改ざん位置検出用の透かし情報が埋め込まれている画像領域Ｂに分離する。本実施形態では、埋め込み装置と同じく、図２に示すように画像領域Ａは最下位（ＬＳＢ）のビットプレーンを除く上位７ビットのビットプレーン２０１とし、画像領域ＢはＬＳＢのビットプレーン２０２とする。このとき画像領域Ｂから得られる画像は画像の改ざんにより、図５の５０２に示すように、改ざん位置で破壊されている可能性がある。

【０１１８】

次に、分離部４０１で分離された画像領域Ｂのデータは、デインターリーバ４０２に入力される。デインターリーバ４０２では、一部が壊れたランダム化された誤り訂正符号化暗号化透かし情報Ｓ’（ＥＣＣ（Ｃ（ｗ））を元のビットの並びに戻す処理を行う。デインターリーバ４０２はランダム化を解除した一部が壊れた誤り訂正符号化暗号化透かし情報、即ちＥＣＣ’（Ｃ（ｗ））を後段の誤り訂正復号化部４０３に出力する。

【０１１９】

なお、誤り訂正符号の種類によっては、埋め込み時にインターリーバを必要としない場合がある。従って、デインターリーバ４０２における処理は必須ではなく、埋め込み時にインターリーバ１０５でＥＣＣ（Ｃ（ｗ））をランダム化した場合にのみ必要となる。

【０１２０】

次に、デインターリーバ４０２から出力されるＥＣＣ’（Ｃ（ｗ））は、誤り

訂正復号部４０３に入力される。誤り訂正復号部４０３では入力された一部が破壊されたＥＣＣ’（Ｃ（ｗ））に対し、誤り訂正復号処理を行い、暗号化された透かし情報Ｃ（ｗ）を後段の暗号復号部４０４に出力する。

【０１２１】

ここで、画像領域Ｂの透かしデータが改ざんにより大きく破壊され、誤り訂正符号が正しく誤り訂正復号が出来ない場合、「改ざん位置の特定はできないが、画像全体が改ざんされている」旨を結果として表示し、処理を中止する。（但し、誤り訂正符号自体に正しく誤り訂正復号できないことを伝える機能を持っている必要がある。）

次に暗号復号部４０４に入力された誤り訂正復号された暗号化透かし情報Ｃ（ｗ）は、暗号化に用いた秘密鍵に対応する公開鍵を入手し、公開鍵暗号方式で公開鍵を用いて暗号化透かし情報Ｃ（ｗ）を復号化し、透かし情報ｗを復元する。

【０１２２】

透かし情報ｗに検査ビットがある場合は、透かし情報ｗを構成する検査ビットの値をチェック（検査ビットが２次元特徴画像のハッシュ値である場合は、透かし情報ｗに含まれる２次元特徴画像からハッシュ値を計算し、透かし情報ｗ中の検査ビットと一致するか否かを比較）することで、正しい秘密鍵で暗号化（署名生成）された暗号化透かし情報Ｃ（ｗ）であるか、異なる秘密鍵で暗号化（署名生成）された暗号化透かし情報Ｃ（ｗ）であるかを識別することが出来る。検査ビットの値が一致しないならば、暗号化透かし情報Ｃ（ｗ）は暗号化（署名生成）が行われた秘密鍵で暗号化されていないことを意味し、「不正な改ざんが行われている」旨を結果表示し、処理を終了する。

【０１２３】

暗号復号部４０４は暗号化が解除された透かし情報ｗ（図８の８０３に相当）の中から、２次元特徴画像およびダイジェストを取り出し、後段の比較部１００６に出力する。このとき、取り出された２次元特徴画像およびダイジェストは夫々、上記原画像に対する相似画像、ハッシュ算出部９０７が計算したダイジェストである。

【０１２４】

次に、特徴抽出部４０５では、分離部４０１から入力される画像領域Ａ（本実施形態では、最下位（ＬＳＢ）のビットプレーンを除く上位７ビットのビットプレーン２０１）に対し、特徴抽出処理を行い、２次元特徴画像を後段の比較部１００６に出力する。

【０１２５】

次に、ハッシュ算出部１００７では、分離部１００１から入力される画像領域Ａのデータをハッシュ関数に入力し、ダイジェストを生成し、後段の比較部１００６に出力する。

【０１２６】

最後に比較部１００６では、暗号復号部１００４から入力される２次元特徴画像およびダイジェストと、特徴抽出部４０５から入力される２次元特徴情報およびハッシュ算出部１００７から入力されるダイジェストを比較する。

【０１２７】

第１の実施形態では、２つの２次元特徴画像の間で差分がわずかである場合には、「画像内容に大きな変更がある改ざんは存在しない」旨までは伝えることが出来るが、僅かな改ざんが存在するか否かまでは判定できなかった。しかし本実施形態では２次元特徴画像に加え、画像領域Ａに対するダイジェストも求めており、画像領域Ａに１ビットでも変更が存在すれば、２つのダイジェストの間で値が異なることから、これらダイジェストを比較することで僅かな改ざんでも検出することが出来る。

【０１２８】

比較部１００６は比較する２つの２次元特徴画像が夫々異なる場合、第１の実施形態と同様の結果を画像の検証者に提示する。また、夫々の２次元特徴画像が同一で夫々のダイジェストが同一の場合には、完全に改ざんが存在しない旨を結果として表示し、夫々の２次元特徴画像が同一で夫々のダイジェストが異なる場合には、検出できない（僅かな）改ざんが存在する旨を結果として表示することが可能である。

【０１２９】

図１１は本実施形態に係る改ざん位置検出処理の流れを示すフローチャートで

ある。図１１を用いて、本実施形態に係る改ざん位置検出処理を順に説明する。

【０１３０】

まずステップＳ１１００で改ざん画像の入力、及び改ざん位置検出を実行する為の種々の情報（公開鍵や誤り訂正符号のパラメータなど）を入手する。

【０１３１】

次にステップＳ１１０１で入力された改ざん画像を画像領域Ａと画像領域Ｂに分離する。

【０１３２】

次にステップＳ１１０２で必要ならば、画像領域Ｂのデータに対し、ランダム化を解除するデインターリーブ処理を実行する。

【０１３３】

そして次に、誤り訂正符号に誤り訂正可能か否かを判定する機能がある場合にはステップＳ１１０３で誤り訂正が可能か否かを判定し、誤り訂正が不可能である場合はステップＳ１１０５に進み、画像全体が改ざんされている旨を表示する。

【０１３４】

ステップＳ１１０３で誤り訂正が可能であると判定された場合、ステップＳ１１０４に進み、誤り訂正復号処理を行い、改ざん処理により壊れた誤り訂正符号化暗号化透かし情報ＥＣＣ’（Ｃ（ｗ））から暗号化透かし情報Ｃ（ｗ）を復元し、ステップＳ１１０６に進む。

【０１３５】

ステップＳ１１０６では、復元された暗号化透かし情報Ｃ（ｗ）に対し、公開鍵を用いて暗号復号処理を行い、透かし情報ｗを復元する。

【０１３６】

次のステップＳ１１０７では、透かし情報ｗの中の検査ビットが一致するかを判定（検査ビットが２次元特徴画像のハッシュ値である場合は、透かし情報ｗに含まれる２次元特徴画像からハッシュ値を計算し、透かし情報ｗ中の検査ビットと一致するか否かを比較）し、一致しない場合には、ステップＳ１１０８に進み、正しい公開鍵で復号されていない旨、或いは正しい秘密鍵で暗号化されておら

ず画像に改ざんが施された旨を表示する。（誤り訂正符号に情報を正しく訂正可能かチェックする機能がなく、正しい誤り訂正復号が行われていない場合、ステップＳ１１０７で検査ビットが正しく復号されない。その場合には画像が改ざんされた旨だけを表示するとよい。）

ステップＳ１１０７で検査ビットが一致する場合は、ステップＳ１１０９に進む。ステップＳ１１０９では透かし情報ｗから２次元特徴画像とダイジェストを抽出する。次のステップＳ１１１０では、画像領域Ａから２次元特徴画像とダイジェストを算出する。

【０１３７】

次にステップＳ１１１１では、ステップＳ１１０９で透かし情報から抽出された２次元特徴画像とステップＳ１１１０で画像領域Ａから算出された２次元特徴画像とを比較する。次にステップＳ１１１２では、２つの２次元特徴画像が一致しているか否かを判断し、一致していなければステップＳ１１１３に進み、図５の５０３～５０６に示すように２つの２次元特徴画像の差分画像や改ざん位置を表示して終了する。

【０１３８】

一方、２つの２次元特徴画像が一致すれば、ステップＳ１１１４に進み、ステップＳ１１０９で透かし情報から抽出されたダイジェストとステップＳ１１１０で画像領域Ａから算出されたダイジェストを比較する。ステップＳ１１１５で２つのダイジェストが一致しているか否かを判断し、一致していなければステップＳ１１１６に進み、「改ざんされているが、大きな改ざんではない」または「改ざんされているが、改ざん位置は特定できない」旨を表示し、終了する。

【０１３９】

ステップＳ１１１５で２つのダイジェストが一致すれば、ステップＳ１１１７に進み、「画像に改ざんが行われていない」旨を画像の検証者に表示し終了する。

【０１４０】

以上、本実施形態では、“アルゴリズム公開”かつ“秘密情報を用いずに画像の改ざん位置判定が可能”かつ“秘密情報を用いずに画像の改ざんの有無が判定

可能”である改ざん位置検出用透かし埋め込み方法および改ざん位置検出方法について詳しく述べた。

【０１４１】

なお、第１および第２の実施形態では、図２に示すように、最下位（ＬＳＢ）のビットプレーンを除く上位７ビットのビットプレーンを画像領域Ａとし、最下位（ＬＳＢ）のビットプレーンを画像領域Ｂとして説明したが、画像領域Ａと画像領域Ｂの選択方法はその限りではない。例えば、画像領域Ｂは下位２ビットのビットプレーンでもよいし、入力画像中の任意のビット位置から改ざん位置検出用電子透かしの埋め込みにより画質を劣化しないように選択してもよい。そのとき画像領域Ａは画像領域Ｂの領域でなく、かつ改ざんを検証したい画像領域のデータとするとよい。

【０１４２】

また、第１および第２の実施形態では、入力画像として８ビットのグレースケール画像を想定したが、各画素８ビットのＲＧＢカラー画像であってもよい。その場合、画像領域Ｂとして各色の最下位（ＬＳＢ）のビットプレーンを用いることも可能である。

【０１４３】

また、第１および第２の実施形態では、２次元特徴画像を１ビットからなる画像として説明したが、２次元特徴画像を暗号化、誤り訂正符号化した場合にも、透かし情報を格納できる画像領域Ｂが存在するなら、多ビットからなる画像であっても構わない。またそのとき、２次元特徴画像は画像領域Ａよりも小さな画像である必要はなく、同じまたはそれ以上の大きさを持っていても構わない。

【０１４４】

［第３の実施形態］

第１と第２の実施形態では、２次元特徴画像に基づく画像領域Ａにおける改ざん位置検出方法について説明したが、第３の実施形態では誤り訂正符号化暗号化透かし情報に基づく画像領域Ｂにおける改ざん位置検出方法について説明する。

【０１４５】

第３の実施形態の特徴は、透かし情報ｗが正しく復号された場合、暗号化透か

し情報Ｃ（ｗ）も正しいと判断できるので、誤り訂正復号化部４０３で暗号化透かし情報Ｃ（ｗ）を得る為に用いた誤りが訂正された元の誤り訂正符号化暗号化透かし情報ＥＣＣ（Ｃ（ｗ））も正しいと判断できることを利用し、誤りが訂正された誤り訂正符号化暗号化透かし情報ＥＣＣ（Ｃ（ｗ））と一部が破壊された誤り訂正符号化暗号化透かし情報ＥＣＣ’（Ｃ（ｗ））とを比較し、埋め込み位置単位で改ざん位置の特定を行う点にある。

【０１４６】

＜改ざん位置検出用電子透かし埋め込み装置＞

改ざん位置検出用電子透かし埋め込み装置については、第１もしくは第２の実施形態と同じであるので、その説明は省略する。

【０１４７】

＜改ざん位置検出装置＞

図１７は本実施形態に係る改ざん位置検出装置の機能構成を示すブロック図である。図１７は図４に示した第２の実施形態に係る改ざん位置検出装置に第２改ざん位置検出部１７００を加え、誤り訂正復号化部４０３が暗号化復号部４０４からの指示に従って改ざん詳細位置検出部１７００に後述するデータを出力する構成となっている。なお図１７において図４，１０と同じ部分については同じ番号を付けている。また、図１７に示した各部はハードウェアにより構成されていても良いし、各部の機能をプログラムにより表現し、コンピュータに読み込ませて実現させても良い。

【０１４８】

以下では、図１７に示す機能構成を備える改ざん位置検出装置について詳しく説明するが、第１の実施形態における改ざん位置検出装置（図４）に第２改ざん位置検出部１７００を追加する構成も可能である。

【０１４９】

図２２は、改ざんが行われた改ざん画像から改ざん位置を判定する処理を説明するための図である。以下、図１７のブロック図に従って、図２２を用いながら、改ざん位置検出装置が行う処理を説明する。

【０１５０】

図２２において２２０１は改竄がなされた画像を示し、２２１０の領域（網掛けされた三日月の形状の領域）が改竄がなされた領域を示す。以下の説明では２２０１に示す改竄画像を例に取り説明するが、各種の改竄画像に対しても以下説明する処理は適用可能である。

【０１５１】

改ざん画像２２０１（入力画像）は、改ざん位置の検証の為、分離部４０１に入力される。分離部４０１では入力画像を画像領域Ａと改ざん位置検出用の透かし情報が埋め込まれている画像領域Ｂに分離する。本実施形態でも上記実施形態と同様に、図２に示すように画像領域Ａは最下位（ＬＳＢ）のビットプレーンを除く上位７ビットのビットプレーン２０１とし、画像領域ＢはＬＳＢのビットプレーン２０２とする。既に述べたように画像領域Ｂには改ざん位置検出用の透かし情報が埋め込まれている。

【０１５２】

このとき画像領域Ｂから得られる画像は画像の改ざんにより、図５の５０２で示したように、改ざん位置５２０で破壊されている可能性がある。

【０１５３】

次に、分離部４０１で分離された画像領域Ｂのデータは、デインターリーバ４０２に入力される。デインターリーバ４０２では、一部が壊れたランダム化された誤り訂正符号化暗号化透かし情報Ｓ’（ＥＣＣ（Ｃ（ｗ））を構成する各ビット列の並びを、を元のビットの並びに戻す処理を行う。

【０１５４】

そしてデインターリーバ４０２は、デインターリーブ処理を施した一部が壊れた誤り訂正符号化暗号化透かし情報、即ちＥＣＣ’（Ｃ（ｗ））を生成し、後段の誤り訂正復号化部４０３に出力する。

【０１５５】

図２２に示す２２０２は、図５の５０２で示した画像領域Ｂに対してデインターリーブ処理を施して得られる、一部が破壊された誤り訂正符号化暗号化透かし情報ＥＣＣ’（Ｃ（ｗ））を２次元画像として表現したものである。改ざんによって破壊されたビット情報は画像２２０２全体に広がっている。

【０１５６】

なお、誤り訂正符号の種類によっては、埋め込み時にインターリーバを必要としない場合がある。従って、デインターリーバ４０２におけるデインターリーブ処理は必須ではなく、改ざん位置検出用電子透かしの埋め込み時にインターリーバ１０５でＥＣＣ（Ｃ（ｗ））にインターリーブ処理を施した場合にのみデインターリーブ処理が必要となる。

【０１５７】

誤り訂正復号化部４０３では入力された一部が破壊されたＥＣＣ’（Ｃ（ｗ））に対して誤り訂正復号処理を行い、暗号化透かし情報Ｃ（ｗ）を後段の暗号復号部４０４に出力する。

【０１５８】

ここで、画像領域Ｂの透かしデータが改ざんにより大きく破壊され、誤り訂正符号化暗号化透かし情報ＥＣＣ’（Ｃ（ｗ））が正しく誤り訂正復号が出来ない場合、「改ざん位置の特定はできないが、画像全体が改ざんされている」旨を結果として表示し、処理を中止する（但し、誤り訂正符号自体に正しく誤り訂正復号できないことを伝える機能を持っている必要がある）。

【０１５９】

一般に誤り訂正復号化部４０３は、誤り訂正符号化時に用いた規則を利用して、一部が破壊された誤り訂正符号化暗号化透かし情報ＥＣＣ’（Ｃ（ｗ））の誤りを訂正し、誤りが訂正された誤り訂正符号化暗号化透かし情報ＥＣＣ（Ｃ（ｗ））を生成する。そして、誤りが訂正された誤り訂正符号化暗号化透かし情報ＥＣＣ（Ｃ（ｗ））から元の情報である暗号化透かし情報Ｃ（ｗ）を取り出す処理を行う。

【０１６０】

図２２の２２０３は２２０２で示した一部が破壊された誤り訂正符号化暗号化透かし情報ＥＣＣ’（Ｃ（ｗ））の誤りを訂正した、誤り訂正符号化暗号化透かし情報ＥＣＣ（Ｃ（ｗ））を２次元画像として表現したものである。

【０１６１】

本実施形態では、誤り訂正復号化部４０３は、誤り訂正復号した暗号化透かし

情報Ｃ（ｗ）を後段の暗号復号部４０４に出力した後も、一部が破壊された誤り訂正符号化暗号化透かし情報ＥＣＣ’（Ｃ（ｗ））と誤りが訂正された誤り訂正符号化暗号化透かし情報ＥＣＣ（Ｃ（ｗ））を保持するとする。

【０１６２】

そして本実施形態では、誤り訂正復号化部４０３は、暗号復号部４０４から制御信号を受けると、一部が破壊された誤り訂正符号化暗号化透かし情報ＥＣＣ’（Ｃ（ｗ））と誤りが訂正された誤り訂正符号化暗号化透かし情報ＥＣＣ（Ｃ（ｗ））を後段の第２改ざん位置検出部１７００に出力する構成をとるとする。

次に暗号復号部４０４では、入力された誤り訂正復号された暗号化透かし情報Ｃ（ｗ）を復号し、透かし情報ｗを復元する。公開鍵暗号方式で暗号化透かし情報Ｃ（ｗ）が暗号化されている場合、暗号化に用いた秘密鍵に対応する公開鍵を入手し、公開鍵を用いて復号処理を行う。

【０１６３】

このとき、第１と第２の実施形態と同様、本実施形態においても、暗号復号部４０４で透かし情報ｗが正しいか検証を行うが、本実施形態では、透かし情報ｗ全体が正しいか検証を行う。従って、検査ビットは透かし情報の一部に対して整合性の検証を行う為の検査ビットではなく、検査ビット自身を除く透かし情報ｗの全てに対して整合性の検証を行う為の検査ビットであるとする。

【０１６４】

既に第１、第２の実施形態でも検査ビットを用いた透かし情報ｗの整合性の検証方法を説明したが、基本的な検証方法は本実施形態においても同様である。即ち、検査ビットが検査ビットを除く透かし情報のハッシュ値である場合、検査ビットを除く透かし情報をハッシュ関数に入力して得られるハッシュ値を、透かし情報の一部である検査ビットの値と比較することで、透かし情報全体の整合性を検証することが出来る。

【０１６５】

改ざん位置検出用電子透かし埋め込み装置の暗号化部９０３において、ブロック暗号方式（ブロック単位で暗号化を実行する暗号方式）を用いて透かし情報を

暗号化する場合、一般に透かし情報ｗはまずブロック単位（鍵長の単位）に分割され、その後ブロック単位で暗号化される。しかし、分割されたブロックが鍵長に満たない単位の情報量である場合、所定の値（例えばを０）をパディングし、暗号化処理を行う。例えば、公開鍵暗号方式の一種であるＲＳＡ暗号方式もブロック暗号に分類され、ブロック単位で暗号化処理を行う。

【０１６６】

このような場合、透かし情報ｗにパディング値を加えて生成された暗号化透かし情報Ｃ（ｗ）が正しいことを検証するには、透かし情報ｗの暗号化時に加えたパディング値についても整合性が取れているか、暗号復号時にチェックする必要がある。その場合、パディング値も透かし情報ｗと同様に扱うとよい。即ち、改ざん位置検出用電子透かし埋め込み装置では、検査ビットは、検査ビット自身を除く透かし情報とパディング値に対するハッシュ値またはチェックサムとし、改ざん位置検出装置の暗号復号部４０４では検査ビット自身を除く透かし情報とパディング値から算出される検査ビットの値と透かし情報中の検査ビットの値を比較し、透かし情報の整合性を検証すればよい。

【０１６７】

以降、説明を簡単にする為、パディング値が存在する場合の処理については説明を省略する。

【０１６８】

一般に暗号技術は解読を困難にする為、入力データの僅かな変化に対し、出力データはランダムに変化するように設計されており、鍵情報がなければその入出力データの対応関係を推測することは困難である。従って、本実施形態においても、透かし情報と検査ビットの整合性を維持させつつ、偽の暗号化透かし情報を意図的に作成することは、暗号化に用いた秘密の鍵（公開鍵暗号方式では秘密鍵、共通鍵暗号方式では共通鍵）の知識なしには非常に困難である。

【０１６９】

従って、暗号化に用いる暗号方式の安全性が保証されていれば、透かし情報ｗと検査ビットの間で整合が取れていないならば、暗号化透かし情報Ｃ（ｗ）に改ざんが行われたとみなし、透かし情報ｗと検査ビットの間で整合が取れているな

らば、暗号化透かし情報Ｃ（ｗ）に改ざんは行われていないと見なす判断を行っても、実用上差し支えないと言える。

【０１７０】

本実施形態では、透かし情報ｗが整合性を満たしていれば、暗号化透かし情報Ｃ（ｗ）、そして暗号化透かし情報Ｃ（ｗ）を得る為に用いた誤りが訂正された誤り訂正符号化暗号化透かし情報ＥＣＣ（Ｃ（ｗ））も正しいと見なす。従って、検証者は秘密の鍵を入手することなく、埋め込みに用いた誤り訂正符号化暗号化透かし情報ＥＣＣ（Ｃ（ｗ））を知ることが出来る。

【０１７１】

第１と第２の実施形態では誤り訂正復号化部４０３は正しい暗号化透かし情報Ｃ（ｗ）を出力するとして簡単に説明を行ったが、実際には誤り訂正復号化部４０３から出力される暗号化透かし情報は必ずしも元の正しい暗号化透かし情報Ｃ（ｗ）と同一であるとは限らない。

【０１７２】

例えば、誤り訂正符号化部１０４が符号化処理を行う際に用いるパラメータは公開されている為、このパラメータを用いて偽造者が誤り訂正復号化部４０３で誤り訂正復号可能なように、偽の暗号化透かし情報を誤り訂正符号化し、偽の誤り訂正符号化暗号化透かし情報を生成して、画像領域Ｂと置き換えた場合を想定してみる。このとき、改ざん位置検出装置の誤り訂正復号化部４０３は、単純に誤り訂正復号を行い、偽の暗号化透かし情報を出力する。

【０１７３】

また、何らかの改ざんを行った結果、偶然に、誤った暗号化透かし情報Ｃ’（ｗ）の誤り訂正符号化情報に相当する誤り訂正符号化暗号化透かし情報ＥＣＣ（Ｃ’（ｗ））が生成される場合もあり得る。

【０１７４】

また誤り訂正符号自体に誤り訂正可能か検出する機能がない場合、誤り訂正復号部４０３は、入力される情報を単純に規則に基づいて誤り訂正復号化し、本来の暗号化透かし情報Ｃ（ｗ）とは全く異なる暗号化透かし情報Ｃ’（ｗ）を出力する場合もある。

【０１７５】

上述のように誤り訂正復号化部４０３から、誤った暗号化透かし情報Ｃ’（ｗ）が出力される様々なケースが想定される。

【０１７６】

しかし、本実施形態では、暗号復号部４０４で暗号化透かし情報を復号後、検査ビットを用いて透かし情報の整合性を検証することで、透かし情報の改ざんを検出することが出来る。

【０１７７】

例えば、検査ビットが検査ビットを除く透かし情報のハッシュ値である場合、暗号復号部４０４では、検査ビットを除く透かし情報をハッシュ関数に入力して得られるハッシュ値を、透かし情報の一部である検査ビットの値と比較し、一致しない場合には、透かし情報、暗号化透かし情報が誤っている、即ち改ざんが加えられていると見なすことが出来る。その場合、改ざん位置は特定できないが画像が改ざんされている旨、或いは改ざんが画像全体に渡っているとして、画像全体が改ざんされている旨を表示してもよい。

【０１７８】

また、第１と第２の実施形態で述べたように、暗号化透かし情報Ｃ（ｗ）が本来暗号化（署名生成）に用いられるべき秘密鍵（例えば、秘密鍵ｐｒｉ１）と異なる秘密鍵（例えば、秘密鍵ｐｒｉ２）で暗号化されている場合、本来用いられるべき秘密鍵（秘密鍵ｐｒｉ１）に対応する公開鍵（公開鍵ｐｕｂ１）を用いて暗号復号を行っても、正しく復号されない。従って、検査ビットを用いて透かし情報の整合性を検証しても、透かし情報の誤りが検出される。この場合も、同様に改ざんが加えられているとし、改ざん位置は特定できないが画像が改ざんされている旨、或いは改ざんが画像全体に渡っているとして、画像全体が改ざんされている旨を表示してもよい。

【０１７９】

また、誤って、暗号化（署名生成）に用いた秘密鍵に対応していない公開鍵を用い、透かし情報ｗの暗号化を復号した場合にも検査ビットの値は一致しない。この場合、「暗号化透かし情報の復号に用いる鍵が異なる」旨を画像の検証者に

通知しても良い。但し、一般に画像の検証者は暗号化の復号の為の鍵を間違わないように注意すべきであり、暗号復号部４０４においても暗号化透かし情報の復号に用いる鍵が誤っていると特定できない場合は、画像に改ざんが加えられていると見なし、改ざん位置は特定できないが画像が改ざんされている旨、或いは改ざんが画像全体に渡っているとして、画像全体が改ざんされている旨を表示してもよい。

【０１８０】

暗号復号部４０４の内部処理において、検査ビットを用いた透かし情報の検証の結果、透かし情報中の検査ビットの値が、検査ビットを除く他の透かし情報から算出される検査ビット（例えばハッシュ値やチェックサム）と一致するならば、暗号復号部４０４は、誤り訂正復号部４０３に対し制御信号を送る。

【０１８１】

誤り訂正復号化部４０３は、暗号復号部４０４からの制御信号を受け、一部が破壊された誤り訂正符号化暗号化透かし情報ＥＣＣ’（Ｃ（ｗ））と誤りが訂正された誤り訂正暗号化透かし情報ＥＣＣ（Ｃ（ｗ））を後段の第２改ざん位置検出部１７００に出力する。

【０１８２】

従って、本実施形態では、誤り訂正復号化部４０３で単純に誤り訂正復号が成功しても、第２改ざん位置検出部１７００は改ざん位置の検出を行わない。

【０１８３】

これは、既に述べたように、誤り訂正復号化部４０３で誤り訂正復号が成功しても、誤り訂正復号化部４０３から必ずしも正しい暗号化透かし情報Ｃ（ｗ）が出力されるとは限らず、誤った暗号化透かし情報Ｃ’（ｗ）が出力される可能性もある。従って、誤り訂正復号化部４０３からの出力データは信頼性が低く、そのデータを元にした改ざん位置検出は信頼性が低いと考えられる為である。

【０１８４】

一方、秘密の鍵（公開鍵暗号方式における秘密鍵、または共通鍵暗号方式における共通鍵）の知識なしに透かし情報ｗの整合性を満たす形で改ざんを行うことは暗号の原理上非常に困難である。従って、透かし情報ｗの整合性を検証できれ

ば、暗号化透かし情報Ｃ（ｗ）は信頼のできるデータであり、信頼のできる暗号化透かし情報Ｃ（ｗ）を再誤り訂正符号化して得られる誤りが訂正された誤り訂正符号化暗号化透かし情報ＥＣＣ（Ｃ（ｗ））も信頼できると考えられる。

【０１８５】

従って、透かし情報ｗの整合性を検証した上で、誤りが訂正された誤り訂正符号化暗号化透かし情報ＥＣＣ（Ｃ（ｗ））と一部を破壊された誤り訂正符号化暗号化透かし情報ＥＣＣ’（Ｃ（ｗ））を比較すれば、正確で誤りのない改ざん位置の特定が可能になると考えられる。

【０１８６】

次に、暗号復号部４０４は暗号化が解除された透かし情報ｗ（例えば、図８の８０３に相当）の中から、２次元特徴画像およびダイジェストを取り出し、後段の比較部１００６に出力する。このとき、取り出された２次元特徴画像およびダイジェストは夫々、上記原画像に対する相似画像、ハッシュ算出部９０７が計算したダイジェストである。

【０１８７】

以降、特徴抽出部４０５、ハッシュ算出部１００７、比較部１００６の動作は、第２の実施形態の動作と同じである。

【０１８８】

次に、特徴抽出部４０５では、分離部４０１から入力される画像領域Ａ（本実施形態では、最下位（ＬＳＢ）のビットプレーンを除く上位７ビットのビットプレーン２０１）に対し、特徴抽出処理を行い、２次元特徴画像を後段の比較部１００６に出力する。

【０１８９】

次に、ハッシュ算出部１００７では、分離部４０１から入力される画像領域Ａのデータをハッシュ関数に入力し、ダイジェストを生成し、後段の比較部１００６に出力する。

【０１９０】

比較部１００６では、暗号復号部４０４から入力される２次元特徴画像およびダイジェストと、特徴抽出部４０５から入力される２次元特徴情報およびハッシ

ュ算出部１００７から入力されるダイジェストを比較する。

【０１９１】

比較部１００６は、比較する２つの２次元特徴画像が夫々異なる場合、第１の実施形態と同様の結果を画像の検証者に提示する。また、夫々の２次元特徴画像が同一で夫々のダイジェストが同一の場合には、画像領域Ａには、完全に改ざんが存在しない旨を結果として表示し、夫々の２次元特徴画像が同一で夫々のダイジェストが異なる場合には、画像領域Ａに位置を検出できない（僅かな）改ざんが存在する旨を結果として表示することが可能である。

【０１９２】

本実施形態では、更に第２改ざん位置検出部１７００を用い、第１、第２の実施形態で述べた画像領域Ａにおける改ざん位置検出に加え、画像領域Ｂにおける改ざん位置検出を実現するが、以下、第２改ざん位置検出部について詳しく説明する。

【０１９３】

図１８は第２改ざん位置検出部１７００の機能構成を示すブロック図である。第２改ざん位置検出部１７００は、第２比較部１８０１、インターリーバ１８０２、埋め込み位置対応部１８０３から成り立っている。以下、各ブロックについて説明する。

【０１９４】

第２比較部１８０１には、誤り訂正復号化部４０３から、誤りが訂正された誤り訂正符号化暗号化透かし情報ＥＣＣ（Ｃ（ｗ））と一部が破壊された誤り訂正符号化暗号化透かし情報ＥＣＣ’（Ｃ（ｗ））が入力される。

【０１９５】

既に述べたが、透かし情報ｗの整合性が既に検証されている為、暗号化透かし情報Ｃ（ｗ）と誤りが訂正された誤り訂正符号化暗号化透かし情報ＥＣＣ（Ｃ（ｗ））は、それぞれ、改ざん位置検出用電子透かし埋め込み装置で生成した暗号化透かし情報Ｃ（ｗ）と誤り訂正符号化暗号化透かし情報ＥＣＣ（Ｃ（ｗ））と全く同一であると見なす。

【０１９６】

第２比較部１８０１では、入力された２つのビット系列、即ち、一部が破壊された誤り訂正符号化暗号化透かし情報ＥＣＣ’（Ｃ（ｗ））と誤りが訂正された誤り訂正符号化暗号化透かし情報ＥＣＣ（Ｃ（ｗ））をビット単位で比較する。

【０１９７】

２つのビット系列が１または０のビットからなる場合、２つのビット系列の簡単な比較は、２つのビット系列で夫々同位置に位置するビット同士のＸＯＲ（排他的論理和）値を算出することで実現できる。２つのビット系列で夫々同位置に位置するビット同士の値が同じであればＸＯＲ値は０、異なればＸＯＲ値は１となる。このようにして、２つのビット系列で対応するビット同士のＸＯＲ値を並べたビット系列（第２改ざん位置特定ビット系列ＢＳ）を求め、後段のインターリーバ１８０３に出力する。ここで第２改ざん位置特定ビット系列ＢＳは一般には、２つのビット系列で互いに異なるビット値であるビットの位置を示すものである。

【０１９８】

図２２の２２０４は第２改ざん位置特定ビット系列ＢＳを２次元画像として表現したもので、図２２の２２０２で示される一部が破壊された誤り訂正符号化暗号化透かし情報と２２０３で示される誤りが訂正された誤り訂正符号化暗号化透かし情報とで、異なるビット値の分布（位置）を示している。２２０４では、改ざんによって破壊されたビットが画像全体に分散して存在している。

【０１９９】

次にインターリーバ１８０２は、入力された第２改ざん位置特定ビット系列ＢＳの並びを並び替え、インターリーブ処理を施した第２改ざん位置特定ビット系列Ｓ（ＢＳ）を生成し、後段の埋め込み位置対応部１８０３に出力する。

【０２００】

このときインターリーバ１８０２が行う処理は、改ざん位置検出用電子透かし埋め込み装置におけるインターリーバ１０５と同一の処理である。既に述べているがインターリーバ１８０２は必須の処理ではなく、改ざん位置検出用電子透かし埋め込み装置でインターリーバを用いた場合にのみ必要となる処理である。

【０２０１】

次に埋め込み位置対応部１８０３では、インターリーブ処理を施した第２改ざん位置特定ビット系列Ｓ（ＢＳ）と入力画像（改ざん画像）における埋め込み位置を対応付ける。

【０２０２】

図２３は、第２改ざん位置特定ビット系列Ｓ（ＢＳ）と改ざん画像との対応を示す図である。一次元配列のビット列である第２改ざん位置特定ビット系列Ｓ（ＢＳ）を２次元配列に並べることで、同図左の２次元ビット配列２３００が得られる。即ち、改ざん画像２２０１のサイズが縦Ｈ画素、横Ｗ画素であるとすると、第２改ざん位置特定ビット系列Ｓ（ＢＳ）も同様に先頭ビットから順番に並べて縦Ｈ画素、横Ｗ画素に配列させることで、２次元ビット配列２３００を得ることができる。このような２次元ビット配列２３００を生成することで、同図右に示した改ざん画像２２０１において改ざん領域２２１０に対応する領域２３０１にビット値”１”が、その他の領域にはビット値”０”が配置されることになる。よって、２次元ビット配列２３００においてビット値が１であるビット位置に対応する改ざん画像２２０１における画素を参照することで、この参照した画素の集合が改ざん領域（２２１０）となる。

【０２０３】

図２２の２２０５はインターリーブ処理を施した第２改ざん位置特定ビット系列Ｓ（ＢＳ）において、改ざん領域２２１０を明示的に示した図である。２２０４では改ざんによって破壊されたビットが画像全体に分散して存在していたが、２２０５では、改ざんによって破壊されたビットが改ざん領域２２１０に集中して存在している。

【０２０４】

第２改ざん位置検出部１７００は、最後に改ざん位置を表示して終了する。このとき、第１や第２の実施形態で既に述べたように改ざん位置を示す差分画像（例えば画像２２０５）を表示してもよいし、図２２の画像２２０６で示すように入力画像に対して差分画像（例えば画像２２０５）をオーバーレイ（重ね合わせ）して改ざん位置を表示しても良い。

【０２０５】

２次元特徴画像の解像度（画像の大きさ）が改ざん画像の解像度よりも低い場合、本実施形態における改ざん位置検出結果（図２２の画像２２０６）の方が第１、第２の実施形態における改ざん位置検出結果（図５の画像５０６）よりも高い解像度（埋め込み位置単位）で改ざん位置の特定を実現していることが分かる。

【０２０６】

以上、デインターリーブ処理を施した一部が破壊された誤り訂正符号化暗号化透かし情報ＥＣＣ’（Ｃ（ｗ）’）と誤りが訂正された誤り訂正符号化暗号化透かし情報ＥＣＣ（Ｃ（ｗ））を比較し、改ざん位置を特定する第２改ざん位置検出部１７００の処理について詳しく述べた。

【０２０７】

なお、本実施形態では、誤り訂正復号化部４０３が、誤りが訂正された誤り訂正暗号化透かし情報ＥＣＣ（Ｃ（ｗ））を生成するとして説明を行ったが、誤り訂正復号化部４０３が、暗号化透かし情報Ｃ（ｗ）のみを出力し、誤りが訂正された誤り訂正暗号化透かし情報ＥＣＣ（Ｃ（ｗ））を外部に出力しない構成をとる場合、誤り訂正復号化部４０３から出力される暗号化透かし情報Ｃ（ｗ）を再び誤り訂正符号化し、誤りが訂正された誤り訂正暗号化透かし情報ＥＣＣ（Ｃ（ｗ））を生成する構成をとってもよい。

【０２０８】

透かし情報ｗが整合性を満たす場合、暗号化透かし情報Ｃ（ｗ）もそれを誤り訂正符号化した誤り訂正符号化暗号化透かし情報ＥＣＣ（Ｃ（ｗ））も正しいと見なすことが出来る。

【０２０９】

暗号化透かし情報Ｃ（ｗ）を再び誤り訂正符号化した誤り訂正暗号化透かし情報ＥＣＣ（Ｃ（ｗ））と一部が破壊された誤り訂正符号化暗号化透かし情報ＥＣＣ（Ｃ（ｗ））と比較することで、同様に正確に改ざん位置を特定することが可能である。

【０２１０】

図１９は本実施形態に係る改ざん位置検出処理の流れを示すフローチャートで

ある。図２０は図１９のステップＡ１（ステップＳ１９１０）の詳細を示すフローチャートで、図２１は図１９のステップＡ２（ステップＳ１９２０）の詳細を示すフローチャートである。

【０２１１】

以下、図１９、図２０、図２１を用いて、本実施形態に係る改ざん位置検出処理について説明する。なお、図１９、図２０中で図１１と同じ番号が記された処理は、図１１と同様の処理を行うとする。

【０２１２】

ステップＳ１１００～ステップＳ１１０６の処理は、第１、第２の実施形態で詳しく述べたのでここでの説明は省略する。

【０２１３】

ステップＳ１１０７では、透かし情報ｗ中の検査ビットを用いて、透かし情報ｗの整合性を検証する。ステップＳ１１０７で検査ビットが一致しない場合（透かし情報ｗが整合性を満たさない場合）には、ステップＳ１１０８に進み、画像に改ざんが施された旨、あるいは、暗号化（署名生成）で用いた秘密鍵と復号で用いた公開鍵が対応していない旨を表示する。

【０２１４】

ステップＳ１１０７で検査ビットが一致する場合は、ステップＡ１（ステップＳ１９１０）に進む。ステップＡ１（ステップＳ１９１０）における処理の詳細は、図１１のステップＳ１１０９～ステップＳ１１１７と同様の処理であり、第２の実施形態で詳しく説明を行った為、説明を省略する。

【０２１５】

次に、ステップＡ１（ステップＳ１９１０）の処理が終了した後、ステップＡ２（ステップＳ１９２０）に移る。ステップＡ２（ステップＳ１９２０）では、図１７の第２改ざん位置検出部１７００における処理が行われる。

【０２１６】

既にステップＳ１１０７で透かし情報ｗ及び暗号化透かし情報Ｃ（ｗ）の整合性が確認されているので、ステップＳ２１０１の制御信号送信処理では、暗号復号部４０４から誤り訂正復号化部４０３に制御信号を送る。

【０２１７】

誤り訂正復号化部４０３はこの制御信号を受けて、後段の第２改ざん位置検出部１７００に一部が破壊された誤り訂正符号化暗号化透かし情報ＥＣＣ’（Ｃ（ｗ））と誤りが訂正された誤り訂正符号化暗号化透かし情報ＥＣＣ（Ｃ（ｗ））を出力する。

【０２１８】

次に、ステップＳ２１０２の比較処理では、既にステップＳ１１０２でデインターリーブ処理された一部が破壊された誤り訂正符号化透かし情報ＥＣＣ’（Ｃ（ｗ））のビット系列とステップＳ１１０４で誤りが訂正された誤り訂正符号化暗号化透かし情報ＥＣＣ（Ｃ（ｗ））のビット系列とを比較し、上記第２改ざん位置特定ビット系列ＢＳを生成する。

【０２１９】

次に、ステップＳ２１０３では、２つのビット系列が一致するか否かを判定する。一致した場合（例えば、２つのビット系列において位置的に対応するビット同士のＸＯＲ値を、全てのビット同士について求め、全てのＸＯＲ値が０である場合）、ステップＳ２１０７に進み、画像領域Ｂに改ざんが存在しない旨を表示し、改ざん位置検出装置の処理を終了する。

【０２２０】

一致しない場合（例えば、２つのビット系列において位置的に対応するビット同士のＸＯＲ値を、全てのビット同士について求め、１であるＸＯＲ値が１つ以上存在する場合）、ステップＳ２１０４に進む。

【０２２１】

次にステップＳ２１０４では、第２改ざん位置特定ビット系列ＢＳに対し、ビット系列の並びを並べ替えるインターリーブ処理を実行し、インターリーブ処理が施された第２改ざん位置特定ビット系列Ｓ（ＢＳ）を生成する。

【０２２２】

なお、ステップＳ２１０４のインターリーブ処理は、改ざん位置検出用電子透かし埋め込み装置においてインターリーバ１０５が存在し、誤り訂正符号化暗号化透かし情報ＥＣＣ（Ｃ（ｗ））に対しインターリーブ処理を行ったときにのみ

必要となる。

【０２２３】

次に、ステップＳ２１０５では、インターリーブ処理が施された第２改ざん位置特定ビット系列Ｓ（ＢＳ）のビットと入力画像中の位置を対応付ける位置対応処理を行う。

【０２２４】

次に、ステップＳ２１０６では、入力画像中の位置と対応付け、改ざん位置の表示を行う。このとき、第１や第２の実施形態で述べたように改ざん位置を入力画像にオーバーレイ（重ね合わせ）して表示してもよいし、その表示方法については限定するものではない。

【０２２５】

ステップＳ２１０６の処理が終了したら、改ざん位置検出装置の処理を終了する。

【０２２６】

なお、図１９ではステップＡ１、ステップＡ２の順序で処理を行う場合について説明したが、ステップＡ１とステップＡ２の処理の順序が逆転していてもよく、ステップＡ２、ステップＡ１の順序で処理を行っても構わない。

【０２２７】

また、上記ステップＡ１，Ａ２のステップＳ１１１３，Ｓ１１１６，Ｓ１１７，Ｓ２１０７，Ｓ２１０６の各ステップにおける処理は、本実施形態では夫々で独自に実行されていたが、まとめて総合的な結果を通知しても良い。

【０２２８】

例えば、ステップＳ１１１３で特定した（２次元特徴画像から求まる）改ざん位置を用いて画像全体の改ざんの概要を示し、ステップＳ２１０６で特定した（第２改ざん位置特定ビット系列ＢＳから求まる）改ざん位置を用いて正確な改ざん位置を示してもよい。また、ステップＳ１１１３で特定した画像領域Ａの改ざん位置とステップＳ２１０６で特定した画像領域Ｂの改ざん位置を統合して表示しても良い。

【０２２９】

第１および第２の実施形態では、２次元特徴画像に基づいて改ざん位置の検出を行う為、２次元特徴画像が入力画像の縦横の解像度よりも小さい場合、改ざん位置の特定は２次元特徴画像の解像度で行っていた。また改ざん位置の特定は画像領域Ａを対象とし、画像領域Ｂを対象としていなかった。

【０２３０】

しかし、本実施形態に係る上記方法を用いれば、２次元特徴画像の解像度に関わらず、画像領域Ｂにおける埋め込み位置単位の正確な改ざん位置検出が可能である。

【０２３１】

従って、第３の実施形態では、第１と第２の実施形態で実現した

（１）　２次元特徴画像を用いた画像領域Ａにおけるロバストな改ざん位置検出

（２）　ダイジェストを用いた画像領域Ａにおける改ざん有無検出

に加え、

（３）　画像領域Ｂにおける埋め込み位置単位の改ざん位置検出

を実現することが可能となる。

【０２３２】

なお、本実施形態では、８ビットグレースケール画像のＬＳＢに改ざん位置検出用の透かしデータを埋め込む場合を例に説明を行ったが、改ざん位置検出用の透かしデータの埋め込みは、ＬＳＢに限らない。

【０２３３】

第７や第８の実施形態でも説明するが、圧縮符号化画像の代表であるＪＰＥＧ圧縮符号化画像やＪＰＥＧ２０００圧縮符号化画像などにおいても適用可能である。

【０２３４】

例えば、ＪＰＥＧ圧縮符号化画像やＪＰＥＧ２０００圧縮符号化画像における量子化後の離散コサイン変換（ＤＣＴ）係数や離散ウェーブレット変換（ＤＷＴ）係数に対し、例えば、量子化後の係数が所定の定数の奇数倍または偶数倍となるように量子化することで、０または１のビット情報を埋め込むことが可能であ

る。例えばある係数の値が５の場合、この係数に”１”を埋め込みたい場合には商が奇数となるような量子化値（第１の量子化値）を用いればよいし、この係数に”０”を埋め込みたい場合には商が偶数となるような量子化値（第２の量子化値）を用いればよい。このような第１の量子化値，第２の量子化値の例としては共に”２”が代表的ではあるが、夫々の量子化値で異なる値を用いても良い。

【０２３５】

このように画像の周波数係数に改ざん位置検出用透かし情報を埋め込む場合、改ざん位置検出装置では、量子化後の周波数係数に基づいた改ざん位置の検出を実現することが出来る。

【０２３６】

また本実施形態で述べた改ざん位置検出装置の特徴は、透かし情報の整合性が確認できれば画像領域Ｂの改ざん位置を検出できることから、透かし情報として画像とは関係のない情報を用いてもよい。

【０２３７】

例えば、予め決められた情報とその情報の検査ビットから透かし情報を構成してもよい。透かし情報としては、改ざん位置検出システム全体で予め決めておいた固定の情報などが考えられる。改ざん位置検出装置の利用者は、暗号復号部で、抽出された透かし情報が予め決められた情報と一致するかを確認し、かつ透かし情報の整合性を確認すれば、透かし情報が改ざんされていないことを確認できる。透かし情報には、特徴画像情報や画像領域Ａのハッシュ値が含まれないため、図１９のステップＡ１の処理は省略されるが、ステップＡ２の処理を実行することで画像領域Ｂの改ざん位置検出は可能であり、このような変形例も改ざん位置検出装置として十分に機能する。

【０２３８】

透かし情報の情報量が少なければ、画像領域Ｂに収まるように暗号化透かし情報に対して冗長な誤り訂正符号化を行うことが出来る。従って、画像の多くの部分が改ざんされた場合にも、誤り訂正復号が可能となり、改ざんに対する耐性、即ち改ざん位置の特定能力を強めることが出来る。

【０２３９】

［第４の実施形態］

第１乃至３の実施形態では、主に２次元特徴画像が各画素１ビットの場合について説明してきた。しかし画像の種類によっては、各画素１ビットの高精細画像（画素数が大きい画像）よりも各画素８ビットなどの多階調画像の方が原画像の雰囲気を良く表すことが出来る場合もある。本実施形態では、特徴抽出部の処理で多階調の画像を生成するようにしてもよい。

【０２４０】

例えば、第１の実施形態では、特徴抽出部は縦２５６画素、横２５６画素の各画素１ビットの２次元特徴画像を生成したが、本実施形態では、縦１２８画素、横１２８画素の各画素４ビットを生成してもよい。このとき透かし情報のデータ量は両者で同一である。

【０２４１】

多階調の２次元特徴画像に対応する場合には、透かし情報ｗの内部に図８の８０４に示すような２次元特徴画像の「階調数」を記録する領域を導入し、２次元特徴画像のデータの並びを定義しておけば、透かし情報から多階調の２次元特徴画像を復元することが可能である。また図示しないが２次元特徴画像を構成する「色情報」なども透かし情報の一部として導入可能である。従って、透かし情報のフォーマットは世間でよく用いられる画像フォーマット（例えばＴＩＦＦやＪＰＥＧなど）と類似の構成をとることが出来る。

【０２４２】

多値の２次元特徴画像を生成する為の処理の一例としては、入力画像に対する縮小処理、離散ウェーブレット変換処理後に低周波成分を取得する処理など、様々な処理が可能である。既に述べたが、特徴抽出処理は透かし情報の中の特徴抽出処理ＩＤに記載しておけば、改竄位置検出装置は改ざん画像から抽出される透かし情報ｗ中の特徴抽出処理ＩＤを元に特徴抽出部で行う特徴抽出処理を知ることが出来る。その為、改ざん位置検出装置の特徴抽出部で特徴抽出処理ＩＤに基づく特徴抽出を実行することで、改ざん位置検出が可能になる。

【０２４３】

［第５の実施形態］

第５の実施形態では、２次元特徴画像のデータ量削減方法について述べる。画像から改ざん位置検出を行う場合、特定の関心領域以外に改ざんが行われていたとしても検出する必要が無い場合もある。例えば、車の画像中で車のナンバープレートの領域しか興味がなく、画像中でナンバープレートの領域に対する改竄の有無や位置の検出のみを行う場合がある。

【０２４４】

この場合、画像全体の情報から２次元特徴画像を計算し、計算した２次元特徴画像全部を透かし情報ｗ内部に配置すると情報量に無駄がある。そのような場合、２次元特徴画像中で最も重要な領域を切り取り、切り取った部分の画像（部分画像）を２次元特徴画像として、透かし情報ｗ内部に配置するとよい。その場合、図示しないが、元の２次元特徴画像の左上隅を原点とする座標において、部分画像の左上隅の座標（ａ１、ａ２）から縦ｐｘ、横ｐｙ（部分画像の縦のサイズがＰｘ、横のサイズがＰｙとする）の画像を各画素８ビットで切り出しているという情報を記録できるように透かし情報のフォーマットを形成すればよい。

【０２４５】

例えば、デジタルカメラで撮影する画像に自動的に透かし情報を埋め込む場合、フォーカスが合った位置を中心とする所定の矩形領域を上記部分画像としておくだけで、透かし情報ｗ内の２次元特徴画像のデータ量を大幅に削減することが出来る。

【０２４６】

更には、２次元特徴画像は画像データである為、得られた２次元特徴画像に対し、様々な圧縮処理を施し、圧縮した２次元特徴画像を透かし情報ｗ内に配置することも可能である。

【０２４７】

上記で述べた２次元特徴画像の抽出処理は特徴抽出処理ＩＤとして、透かし情報ｗ内に記録することで、改ざん位置検出時にも同様の２次元特徴画像を生成することが出来る。

【０２４８】

[第６の実施形態]

第１～第５の実施形態では、特徴抽出部では単一の特徴抽出処理を用いて、２次元特徴画像を生成する処理について述べたが、第６の実施形態では、特徴抽出部では複数の特徴抽出処理を用いて複数の２次元特徴画像を生成する。

【０２４９】

特徴抽出部で単一の特徴抽出処理を行い２次元特徴画像を生成する場合、改ざんの前後における２次元特徴画像に差がない場合には改ざん位置まで検出することが難しかった。

【０２５０】

しかし、複数の特徴抽出処理を行えば、いずれかの特徴抽出処理で生成される２次元特徴画像において改ざんの前後で差が発生するならば、改ざん位置の検出が可能になる。

【０２５１】

本実施形態では、複数の特徴抽出処理から得られる複数の２次元特徴画像を埋め込み装置と改竄位置検出装置の双方で求め、同じ抽出処理を用いて得られた画像同士を比較することで、第１～第５の実施形態で検出できなかった画像の改ざん位置をより検出しやすくする効果がある。

【０２５２】

例えば、簡単な一例として、第１の特徴抽出部は離散ウェーブレット変換の低周波成分（ＬＬ）に基づく２次元特徴画像を抽出するとし、第２の特徴抽出部は離散ウェーブレット変換の高周波成分（ＨＨ）に基づく２次元特徴画像を抽出するとよい。２次元特徴画像は、画像領域Ｂの情報量に応じて、画像領域Ｂに収まるように階調数を減らす必要があるが、低周波成分と高周波成分の両方を２次元特徴画像に含ませることで、双方において改ざん前後で変化しない改ざん画像を生成することを難しくし、画像の改ざん位置を検出し易くすることが出来る。

【０２５３】

また、第１の特徴抽出部は多値の縮小画像を２次元特徴画像として抽出するとし、第２の特徴抽出部は画像の輪郭を２次元特徴画像として抽出するとする。この場合にも、画像全体で平均値を維持しつつ、輪郭を変化がすることのない改ざん画像を生成することは難しく、画像の改ざん位置をより検出し易くすることが

出来る。

【０２５４】

その場合、透かし情報には夫々の２次元特徴画像が含まれていると共に、夫々の２次元特徴画像がどのような処理により生成されたものであるかを示す情報が含まれている。

【０２５５】

そして改竄位置検出装置は、改竄画像に対して同様に複数の２次元特徴画像を生成し、透かし情報から抽出した夫々の２次元特徴画像と、改竄画像から生成された夫々の２次元特徴画像とで夫々対応する画像同士（同じ抽出処理により得られた画像同士）を比較することで、改竄の位置を検出することができる。

【０２５６】

なお、本実施形態に係る処理は、上記各実施形態に適用しても良い。

【０２５７】

［第７の実施形態］

本実施形態では、改ざん位置検出用電子透かしの埋め込みを行う画像データがＪＰＥＧ圧縮符号化データである場合について考える。ＪＰＥＧ圧縮符号化方式は、既によく知られている符号化方式の為、詳しい説明はここでは省略する。

【０２５８】

図１２は画像の一部（８×８画素）の領域に対して、離散コサイン変換を実行し、所定の量子化テーブルで量子化したＤＣＴ量子化係数を２次元的に表している図である。

【０２５９】

同図に示した各係数配置において、左上には直流成分（ＤＣ，８×８画素の平均値）が配置されており、その他の位置には夫々固有の周波数成分が配置されている。

【０２６０】

ＪＰＥＧ圧縮符号化データに対して、第１～第４の実施形態で述べた改ざん位置検出用電子透かしを埋め込む場合、各８×８ブロックにおいて、画質への影響が少ない周波数成分を電子透かしの埋め込み対象である画像領域Ｂとしてランダ

ムに１つもしくは複数選択し、残りの領域を画像領域Ａするとよい。例えば、図１２のように１２０２は画像領域Ｂ、その他の周波数成分は画像領域Ａとすることが出来る。

【０２６１】

２次元特徴画像を生成する際には画像領域Ａの中で直流成分（ＤＣ成分）のみを処理の対象として２値画像を生成し、ダイジェストを生成する際には画像領域Ａにある全てのデータを利用するとよい。この場合、ＪＰＥＧ圧縮符号化画像で輝度や色の変更が起きた場合でも、改ざん位置の特定を行うことが可能である。

【０２６２】

［第８の実施形態］

本実施形態では、改ざん位置検出用電子透かしの埋め込みを行う画像データがＪＰＥＧ２０００圧縮符号化画像データである場合について考える。

【０２６３】

ＪＰＥＧ２０００圧縮符号化方式は既によく知られている符号化方式の為、詳しい説明はここでは省略する。ＪＰＥＧ２０００圧縮符号化方式では、入力画像夫々所定のサイズを有するタイルに分割し、タイル単位で離散ウェーブレット変換（ＤＷＴ）を行い、複数の周波数帯域のサブバンドに分割する。図１３は注目タイルに対して離散ウェーブレット変換を行うことで得られるＤＷＴ係数の配置を示す図である。左上のＬＬは画像に最も影響の大きい低周波成分を表すサブバンド、右下のＨＨは画像に影響が少ない高周波成分を表すサブバンドである。

【０２６４】

ＪＰＥＧ２０００圧縮符号化画像データに第１～第６の実施形態で述べた改ざん位置検出用電子透かしの埋め込みを行う一例を述べると、画像領域ＢとしてＬＬの最下位ビットプレーンを選択し、画像領域ＡとしてＬＬの最下位ビットプレーンを除くビットプレーンとして選択するとよい。この場合、ＬＬを複数のビットプレーンからなる２次元画像とみなすことが出来るから、第１や第２の実施形態とほぼ同様に改ざん位置検出用電子透かしの埋め込みと改ざん位置検出が実現できる。ＬＬを操作する場合、画質劣化を生み易いが、高周波のサブバンドを取り除く圧縮に対しても改ざん位置を特定できる機能を維持することが出来る。

【０２６５】

また、その他の埋め込み方法として、画像領域ＢとしてＬＬを除く他の全てのサブバンド（ＨＬ１、ＨＨ１、ＬＨ１、ＨＬ２、ＨＨ２、ＬＨ２）とし、ＬＬそのもの又はＬＬから得られる２次元特徴画像を画像領域Ｂに埋め込んでもよい。画像領域Ｂとしては、LLを除く他の全てのサブバンドではなく、（ＨＬ１、ＨＨ１、ＬＨ１、ＨＬ２、ＨＨ２、ＬＨ２）の中から所定のビットプレーンを選択する形としてもよい。画像領域Ｂに収める情報量が減るが、画像に対する劣化が抑えられるメリットがある。

【０２６６】

また、離散ウェーブレット変換を実行する最小単位であるタイル単位毎に画像領域Ａおよび画像領域Ｂを選択して、改ざん位置検出用電子透かしの埋め込みと改ざん位置検出を行ってもよいが、タイル単位ごとではなく画像全体の複数のタイルにまたがる形で、画像領域Ａおよび画像領域Ｂを選択し、改ざん位置検出用電子透かしの埋め込みと改ざん位置検出を行ってもよい。

【０２６７】

例えば、複数のタイルからＬＬのみを抽出し、最下位のビットプレーンを除く領域を画像領域Ａ、最下位のビットプレーンを画像領域Ｂと設定する。この場合、既に第１乃至３の実施形態で述べたように、画像領域Ａから２次元特徴画像を生成し、透かし情報を生成し、透かし情報に対し暗号化処理、誤り訂正符号化処理、インターリーブ処理を行うことで得られる透かし情報を画像領域Ｂと置き換えればよい。

【０２６８】

［第９の実施形態］

本実施形態では、改ざん位置検出用電子透かしの埋め込みを行う画像データがＭＰＥＧやＭｏｔｉｏｎＪＰＥＧ、ＭｏｔｉｏｎＪＰＥＧ２０００に代表される動画像データである場合について考える。ＭＰＥＧは基本的にはＪＰＥＧ圧縮符号化で用いた離散コサイン変換に基づく圧縮をベースとしており、第７の実施形態で述べたＪＰＥＧ圧縮符号化画像の改ざん位置検出用電子透かしの埋め込み方法を、時間軸に拡張し、画質への影響が少ないＤＣＴ係数を適当に選択すること

により、適用可能である。

【０２６９】

ＭｏｔｉｏｎＪＰＥＧやＭｏｔｉｏｎＪＰＥＧ２０００は、基本的にはＪＰＥＧやＪＰＥＧ２０００圧縮符号化画像を時間軸に重ねた構成となっており、第５、第６の実施形態で述べた手法を時間軸に拡張すれば、簡単に適用することが可能である。

【０２７０】

また上記実施形態に係る処理の対象として音声データを用いても良く、その場合、２次元特徴画像を１次元特徴データに置き換えることで適応可能である。

【０２７１】

［第１０の実施形態］

本実施形態では、上記第１乃至９の実施形態に係る夫々の処理をコンピュータにより行わせる。図１４は、上記第１乃至９の実施形態に係る埋め込み装置、改竄位置検出装置として機能するコンピュータの基本構成を示す図である。例えばこのコンピュータを第１乃至３の実施形態に係る埋め込み装置、改竄位置検出装置として機能させる場合、図１，４，９，１０、１７に示した各機能構成をプログラムにより表現し、このコンピュータに読み込ませることで、このコンピュータを第１乃至３の実施形態に係る埋め込み装置、改竄位置検出装置として機能させることができる。

【０２７２】

また、埋め込み装置、改竄位置検出装置は夫々同一の装置としても良いし、別個の装置としても良い。

【０２７３】

同図において、１４１１はＣＰＵで、ＲＡＭ１４１２やＲＯＭ１４１３に格納されているプログラムやデータを用いて、コンピュータ全体の制御を行うと共に、上記各実施形態で説明した各処理を行う。

【０２７４】

１４１２はＲＡＭで、外部記憶装置１４１８からロードされたプログラムやデータ、他のコンピュータシステム１４２４からＩ／Ｆ（インターフェース）１４

２３を介してダウンロードしたプログラムやデータを一時的に記憶するエリアを備えると共に、ＣＰＵ１４１１が各種の処理を行うために必要とするエリアを備える。

【０２７５】

１４１３はＲＯＭで、コンピュータの機能プログラムや設定データなどを記憶する。１４１４はディスプレイ制御装置で、画像や文字等をディスプレイ１４１５に表示させるための制御処理を行う。１４１５はディスプレイで、画像や文字などを表示する。なお、ディスプレイとしてはＣＲＴや液晶画面などが適用可能である。

【０２７６】

１４１６は操作入力デバイスで、キーボードやマウスなど、ＣＰＵ１４１１に各種の指示を入力することのできるデバイスにより構成されている。なお手動で上記秘密鍵や公開鍵などを入力する場合には、この操作入力デバイス１４１６を介してこれらを入力することができる。１４１７は操作入力デバイス１４１６を介して入力された各種の指示等をＣＰＵ１４１１に通知するためのＩ／Ｏである。

【０２７７】

１４１８はハードディスクなどの大容量情報記憶装置として機能する外部記憶装置で、ＯＳ（オペレーティングシステム）や上記各実施形態に係る処理をＣＰＵ１４１１に実行させるためのプログラム、埋め込み情報を埋め込む対象となる画像データなどを記憶する。また、秘密鍵を予め保存しておいても良い。外部記憶装置１４１８への情報の書き込みや外部記憶装置１４１８からの情報の読み出しはＩ／Ｏ１４１９を介して行われる。

【０２７８】

１４２１は画像を撮像するためのディジタルカメラで、撮像した画像はＩ／Ｏ１４２２を介してＲＡＭ１４１２に出力、もしくは外部記憶装置１４１８に保存される。なお、画像を撮像するための機器はディジタルカメラに限定されるものではなく、例えば動画像を撮像するディジタルビデオカメラであってもよい。

【０２７９】

１４３０はＣＰＵ１４１１、ＲＯＭ１４１３、ＲＡＭ１４１２、Ｉ／Ｏ１４２２、Ｉ／Ｏ１４１９，ディスプレイ制御装置１４１４、Ｉ／Ｆ１４２３、Ｉ／Ｏ１４１７を繋ぐバスである。

【０２８０】

また、改ざん位置検出用電子透かし埋め込み・および改ざん位置検出を行う対象が音声信号の場合、ディジタルカメラ１４２１の代わりにマイク等の音声入力機器をＩ／Ｏ１４２２に接続する。

【０２８１】

なお本実施形態では、改ざん位置検出用電子透かしの埋め込み処理、改竄位置検出処理はコンピュータにより行っているが、改ざん位置検出用電子透かし埋め込み処理を、ディジタルカメラ１４２１によって、専用のハードウェア回路を用いてディジタルデータの撮影直後に行わせ、ＣＰＵ１４１１が改竄位置検出処理を行っても良い。もちろん、ディジタルカメラ１４２１が改ざん位置検出用電子透かしの埋め込み処理を行ってもよい。

【０２８２】

または、図示しないが音声に改ざん位置検出用電子透かしを埋め込む場合、音声入力機器に改ざん位置検出用電子透かしの埋め込み処理を行わせても良い。

【０２８３】

上記各実施形態によれば、画像や動画、音声データに秘密の情報を用いることなく画像や動画、音声データの改ざん位置および改ざんの有無を検出することを可能にする。

【０２８４】

なお、上記各実施形態は、何れも本発明を実施するにあたっての具体化の例を示したものに過ぎず、これらによって本発明の技術的範囲が限定的に解釈されてはならないものである。すなわち、本発明はその技術思想、またはその主要な特徴から逸脱することなく、様々な形で実施することができる。

【０２８５】

［その他の実施形態］

尚、本実施形態は、複数の機器（例えば、ホストコンピュータ、インタフェー

ス機器、リーダ、プリンタ等）から構成されるシステムに適用しても、一つの機器からなる装置（例えば、複写機、ファクシミリ装置等）に適用してもよい。

【０２８６】

また、本発明の目的は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記録媒体（または記憶媒体）を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはＣＰＵやＭＰＵ）が記録媒体に格納されたプログラムコードを読み出し実行することによっても、達成されることは言うまでもない。この場合、記録媒体から読み出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記録した記録媒体は本実施形態を構成することになる。また、コンピュータが読み出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているオペレーティングシステム（ＯＳ）などが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【０２８７】

さらに、記録媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張カードやコンピュータに接続された機能拡張ユニットに備わるメモリに書込まれた後、そのプログラムコードの指示に基づき、その機能拡張カードや機能拡張ユニットに備わるＣＰＵなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【０２８８】

本実施形態を上記記録媒体に適用する場合、その記録媒体には、先に説明したフローチャートや機能構成に対応するプログラムコードが格納されることになる。

【０２８９】

以下に、本発明の実施態様の例を示す。

【０２９０】

［実施態様１］　第１の領域と第２の領域とで構成される原画像に対する改竄の位置を検出可能にするための情報を生成する画像処理装置であって、

前記第１の領域の画像を用いて、前記原画像の特徴画像を生成する特徴画像生成手段と、

前記特徴画像と前記原画像に関する情報とを含む透かし情報を生成する透かし情報生成手段と、

前記透かし情報に対して誤り訂正符号化を行い、誤り訂正符号化透かし情報を生成する誤り訂正符号化手段と、

前記原画像において、前記第２の領域の画像情報を前記誤り訂正符号化透かし情報に置き換えた画像を出力画像として出力する出力手段と

を備えることを特徴とする画像処理装置。

【０２９１】

［実施態様２］　更に、前記透かし情報生成手段が生成した透かし情報を暗号化する暗号化手段を備え、

前記誤り訂正符号化手段は、前記暗号化手段によって暗号化された透かし情報に対して誤り訂正符号化を行うことを特徴とする実施態様１に記載の画像処理装置。

【０２９２】

［実施態様３］　前記暗号化手段は、前記透かし情報を公開鍵暗号化方式に従って暗号化することを特徴とする実施態様２に記載の画像処理装置。

【０２９３】

［実施態様４］　更に、前記誤り訂正符号化透かし情報を構成するビット列を並び替える並び替え手段を備え、

前記誤り訂正符号化透かし情報は前記並び替え手段によってビット列が並び替えられたものであることを特徴とする実施態様２に記載の画像処理装置。

【０２９４】

［実施態様５］　更に、前記第１の領域の画像を用いて、ハッシュ値を計算するハッシュ値計算手段を備え、

前記透かし情報生成手段は、前記透かし情報に更に前記ハッシュ値のデータを

含めることを特徴とする実施態様１乃至４の何れか１項に記載の画像処理装置。

【０２９５】

［実施態様６］　前記原画像に関する情報には、前記透かし情報が正しく復号されたか否かをチェックするために使用されるビット列が含まれることを特徴とする実施態様１に記載の画像処理装置。

【０２９６】

［実施態様７］　前記ビット列は少なくとも前記特徴画像を含む透かし情報の一部に対するハッシュ値であることを特徴とする実施態様６に記載の画像処理装置。

【０２９７】

［実施態様８］　前記原画像に関する情報には、前記特徴画像を生成する処理を特定する情報が含まれることを特徴とする実施態様１に記載の画像処理装置。

【０２９８】

［実施態様９］　前記特徴画像生成手段は、夫々異なる特徴抽出処理を行って前記原画像の特徴画像を複数生成することを特徴とする実施態様１に記載の画像処理装置。

【０２９９】

［実施態様１０］　前記特徴画像は、前記原画像の部分画像であることを特徴とする実施態様１に記載の画像処理装置。

【０３００】

［実施態様１１］　第１の領域と第２の領域とで構成される改竄画像中の改竄の位置を検出する画像処理装置であって、

前記第２の領域に基づいた画像に対して誤り訂正復号を行い、前記改竄画像の改竄前の特徴を表す特徴画像と前記改竄画像の改竄前の画像に関する情報とを含む透かし情報を復元する誤り訂正復号手段と、

前記第１の領域の画像を用いて、前記改竄画像の特徴画像を生成する特徴画像生成手段と、

前記透かし情報に含まれる前記改竄画像の改竄前の特徴を表す特徴画像と、前

記改竄画像の特徴画像とを用いて、前記改竄画像中の改竄の位置を通知する改竄位置通知手段と

を備えることを特徴とする画像処理装置。

【０３０１】

［実施態様１２］　更に、前記第２の領域に基づいた画像を構成する、並び替えられたビット列を元の配置に復元する並び替え手段を備え、

前記誤り訂正復号手段は、前記並び替え手段によって並び替えられた前記第２の領域に基づいた画像に対して誤り訂正復号を行うことを特徴とする実施態様１１に記載の画像処理装置。

【０３０２】

［実施態様１３］　前記誤り訂正復号手段が復号した透かし情報が暗号化されている場合、当該暗号化されている透かし情報を復号し、当該透かし情報を復元する復元手段を備えることを特徴とする実施態様１１又は１２に記載の画像処理装置。

【０３０３】

［実施態様１４］　前記復元手段は、前記暗号化された透かし情報を公開鍵暗号化方式に従って復号することを特徴とする実施態様１３に記載の画像処理装置。

【０３０４】

［実施態様１５］　前記改竄位置通知手段は、前記改竄画像の改竄前を表す画像と前記特徴画像との差分画像を生成し、当該差分画像を用いて前記改竄画像中の改竄の位置を通知することを特徴とする実施態様１１又は１２に記載の画像処理装置。

【０３０５】

［実施態様１６］　更に、前記第１の領域の画像を用いて、ハッシュ値を計算するハッシュ値計算手段と、

前記ハッシュ値計算手段が計算したハッシュ値のデータと前記透かし情報に含まれるハッシュ値のデータとを比較し、前記改竄画像における改竄の有無を通知する改竄有無通知手段と

を備えることを特徴とする実施態様１１に記載の画像処理装置。

【０３０６】

［実施態様１７］　前記改竄画像の改竄前の画像に関する情報には、前記暗号化されている透かし情報に対する改ざんの有無を判断するために、前記透かし情報の一部を検証する際に用いられるビット列が含まれることを特徴とする実施態様１３に記載の画像処理装置。

【０３０７】

［実施態様１８］　前記ビット列は少なくとも前記改竄画像の改竄前の特徴を表す特徴画像を含む透かし情報の一部に対するハッシュ値であることを特徴とする実施態様１７に記載の画像処理装置。

【０３０８】

［実施態様１９］　前記改竄画像に関する情報には、前記透かし情報に含まれる前記改竄画像の改竄前の特徴を表す特徴画像を生成する処理を特定する情報が含まれることを特徴とする実施態様１１に記載の画像処理装置。

【０３０９】

［実施態様２０］　前記透かし情報に含まれる前記改竄画像の改竄前の特徴を表す特徴画像は、前記改竄画像の改竄前の部分画像であって、前記改竄画像の改竄前の画像に関する情報には、前記部分画像に関する情報が含まれることを特徴とする実施態様１１に記載の画像処理装置。

【０３１０】

［実施態様２１］　前記特徴画像生成手段は、夫々異なる特徴抽出処理を行って前記第１の領域の画像の特徴画像を複数生成し、

前記改竄位置通知手段は、前記透かし情報に含まれる前記改竄画像の改竄前を表す夫々の画像と、前記特徴画像生成手段が生成した夫々の特徴画像とで、夫々対応する画像を用いて、前記改竄画像中の改竄の位置を通知することを特徴とする実施態様１２に記載の画像処理装置。

【０３１１】

［実施態様２２］　前記改竄画像の改竄前の画像に関する情報には、当該情報を除く前記透かし情報全部の整合性を検証するためのビット列が含まれること

を特徴とする実施態様１３に記載の画像処理装置。

【０３１２】

［実施態様２３］　前記ビット列は少なくとも前記改竄画像の改竄前の画像に関する情報を除く前記透かし情報全部に対するハッシュ値であることを特徴とする実施態様２２に記載の画像処理装置。

【０３１３】

［実施態様２４］　更に、

前記ビット列を用いて、前記透かし情報に対する改ざんの有無を検出する検出手段と、

前記透かし情報に対する改ざんが検出されなかった場合に、前記誤り訂正復号手段によって誤り訂正される前の第１の暗号化されている透かし情報と、前記誤り訂正復号手段によって誤り訂正された後の第２の暗号化されている透かし情報とで対応するビット同士で、互いに異なるビット値であるビット同士の位置を示す比較画像を生成する比較手段と、

前記比較画像に基づき、前記改竄画像における改ざんの位置を通知する改竄位置通知手段と

を備えることを特徴とする実施態様２２に記載の画像処理装置。

【０３１４】

［実施態様２５］　第１の領域と第２の領域とで構成される原画像に対する改竄の位置を検出可能にするための情報を生成する画像処理装置であって、

予め作成された透かし情報を暗号化し、暗号化透かし情報を生成する暗号化手段と、

前記暗号化透かし情報に対して誤り訂正符号化を行い、誤り訂正符号化暗号化透かし情報を生成する誤り訂正符号化手段と、

前記原画像において、前記第２の領域の画像情報を前記誤り訂正符号化暗号化透かし情報に置き換えた画像を出力画像として出力する出力手段と

を備えることを特徴とする画像処理装置。

【０３１５】

［実施態様２６］　前記暗号化手段は、前記透かし情報を公開鍵暗号化方式

に従って暗号化することを特徴とする実施態様２５に記載の画像処理装置。

【０３１６】

［実施態様２７］　更に、前記誤り訂正符号化透かし情報を構成するビット列を並び替える並び替え手段を備え、

前記誤り訂正符号化透かし情報は前記並び替え手段によってビット列が並び替えられたものであることを特徴とする実施態様２５に記載の画像処理装置。

【０３１７】

［実施態様２８］　前記透かし情報には、前記透かし情報が正しく復号されたか否かをチェックするために使用されるビット列が含まれることを特徴とする実施態様２５に記載の画像処理装置。

【０３１８】

［実施態様２９］　前記ビット列は少なくとも前記特徴画像を含む透かし情報の一部に対するハッシュ値であることを特徴とする実施態様２８に記載の画像処理装置。

【０３１９】

［実施態様３０］　第１の領域と第２の領域とで構成される改竄画像中の改竄の位置を検出する画像処理装置であって、

前記第２の領域に基づいた画像に対して誤り訂正復号を行い、誤りが訂正された第２の領域に基づいた画像を生成し、暗号化透かし情報を復元する誤り訂正復号手段と、

前記暗号化透かし情報を復号し、透かし情報を復元する暗号化復号手段と、

前記透かし情報の整合性を検証する透かし情報検証手段と、

前記透かし情報が整合性を満たしていれば、前記第２の領域に基づいた画像と誤りが訂正された第２の領域に基づいた画像を比較し、改ざん位置を検出する改ざん位置検出手段と

を備えることを特徴とする画像処理装置。

【０３２０】

［実施態様３１］　更に、前記第２の領域に基づいた画像を構成する、並び替えられたビット列を元の配置に復元する並び替え手段を備え、

前記誤り訂正復号手段は、前記並び替え手段によって並び替えられた前記第２の領域に基づいた画像に対して誤り訂正復号を行うことを特徴とする実施態様３０に記載の画像処理装置。

【０３２１】

［実施態様３２］　前記暗号化復号手段は、前記暗号化された透かし情報を公開鍵暗号化方式に従って復号することを特徴とする実施態様３０に記載の画像処理装置。

【０３２２】

［実施態様３３］　第１の領域と第２の領域とで構成される原画像に対する改竄の位置を検出可能にするための情報を生成する画像処理方法であって、

前記第１の領域の画像を用いて、前記原画像の特徴画像を生成する特徴画像生成工程と、

前記特徴画像と前記原画像に関する情報とを含む透かし情報を生成する透かし情報生成工程と、

前記透かし情報に対して誤り訂正符号化を行い、誤り訂正符号化透かし情報を生成する誤り訂正符号化工程と、

前記原画像において、前記第２の領域の画像情報を前記誤り訂正符号化透かし情報に置き換えた画像を出力画像として出力する出力工程と

を備えることを特徴とする画像処理方法。

【０３２３】

［実施態様３４］　第１の領域と第２の領域とで構成される改竄画像中の改竄の位置を検出する画像処理方法であって、

前記第２の領域に基づいた画像に対して誤り訂正復号を行い、前記改竄画像の改竄前の特徴を表す特徴画像と前記改竄画像の改竄前の画像に関する情報とを含む透かし情報を復元する誤り訂正復号工程と、

前記第１の領域の画像を用いて、前記改竄画像の特徴画像を生成する特徴画像生成工程と、

前記透かし情報に含まれる前記改竄画像の改竄前の特徴を表す特徴画像と、前記改竄画像の特徴画像とを用いて、前記改竄画像中の改竄の位置を通知する改竄

位置通知工程と

を備えることを特徴とする画像処理方法。

【０３２４】

[実施態様３５]　第１の領域と第２の領域とで構成される原画像に対する改竄の位置を検出可能にするための情報を生成する画像処理方法であって、

予め作成された透かし情報を暗号化し、暗号化透かし情報を生成する暗号化工程と、

前記暗号化透かし情報に対して誤り訂正符号化を行い、誤り訂正符号化暗号化透かし情報を生成する誤り訂正符号化工程と、

前記原画像において、前記第２の領域の画像情報を前記誤り訂正符号化暗号化透かし情報に置き換えた画像を出力画像として出力する出力工程と

を備えることを特徴とする画像処理方法。

【０３２５】

[実施態様３６]　第１の領域と第２の領域とで構成される改竄画像中の改竄の位置を検出する画像処理方法であって、

前記第２の領域に基づいた画像に対して誤り訂正復号を行い、誤りが訂正された第２の領域に基づいた画像を生成し、暗号化透かし情報を復元する誤り訂正復号工程と、

前記暗号化透かし情報を復号し、透かし情報を復元する暗号化復号工程と、

前記透かし情報の整合性を検証する透かし情報検証工程と、

前記透かし情報が整合性を満たしていれば、前記第２の領域に基づいた画像と誤りが訂正された第２の領域に基づいた画像を比較し、改ざん位置を検出する改ざん位置検出工程と

を備えることを特徴とする画像処理方法。

【０３２６】

[実施態様３７]　コンピュータを実施態様１乃至３２の何れか１項に記載の画像処理装置として機能させることを特徴とするプログラム。

【０３２７】

[実施態様３８]　コンピュータに実施態様３３乃至３６のいずれか１項に

記載の画像処理方法を実行させることを特徴とするプログラム。

【０３２８】

[実施態様３９]　実施態様３７又は３８に記載のプログラムを格納することを特徴とするコンピュータ読み取り可能な記憶媒体。

【０３２９】

【発明の効果】

以上の説明により、本発明によって、画像に対する改竄の位置を正確に検出することができる。

【図面の簡単な説明】

【図１】

本発明の第１の実施形態に係る改ざん位置検出用電子透かし埋め込み装置の機能構成を示すブロック図である。

【図２】

１画素が８ビットから成る入力画像をビットプレーン毎に示した図である。

【図３】

入力画像、２次元特徴画像、そして後述するランダム化された誤り訂正符号化暗号化透かし情報によって表現される画像を示す図である。

【図４】

改ざん位置検出装置の機能構成を示すブロック図である。

【図５】

改ざんが行われた改ざん画像から改ざん位置を判定する処理を説明するための図である。

【図６】

透かし情報（６０１）、暗号化透かし情報（６０２）、誤り訂正符号化透かし情報（６０３）、ランダム化誤り訂正符号化透かし情報（６０４）のビット長を比較、説明するための概略図である。

【図７】

誤り訂正符号化を行う前の透かし情報Ｃ（ｗ）の一例を示す図である。

【図８】

「透かし情報」の概略構成を示す図である。

【図９】

本発明の第２の実施形態に係る改ざん位置検出用電子透かし埋め込み装置の機能構成を示すブロック図である。

【図１０】

本発明の第２の実施形態に係る改ざん位置検出装置の機能構成を示すブロック図である。

【図１１】

本発明の第２の実施形態に係る改ざん位置検出処理の流れを示すフローチャートである。

【図１２】

画像の一部（８×８画素）の領域に対して、離散コサイン変換を実行し、所定の量子化テーブルで量子化したＤＣＴ量子化係数を２次元的に表している図である。

【図１３】

注目タイルに対して離散ウェーブレット変換を行うことで得られるＤＷＴ係数の配置を示す図である。

【図１４】

本発明の第１乃至８の実施形態に係る埋め込み装置、改竄位置検出装置として機能するコンピュータの基本構成を示す図である。

【図１５】

論文（１）における改ざん位置検出用電子透かし埋め込み装置の機能構成を示すブロック図である。

【図１６】

論文（１）における改ざん位置検出装置の機能構成を示すブロック図である。

【図１７】

本発明の第３の実施形態に係る改ざん位置検出装置の機能構成を示すブロック図である。

【図１８】

第２改ざん位置検出部１７００の機能構成を示すブロック図である。

【図１９】

本発明の第３の実施形態に係る改ざん位置検出処理の流れを示すフローチャートである。

【図２０】

図１９のステップＡ１（ステップＳ１９１０）の詳細を示すフローチャートである。

【図２１】

図１９のステップＡ２（ステップＳ１９２０）の詳細を示すフローチャートである。

【図２２】

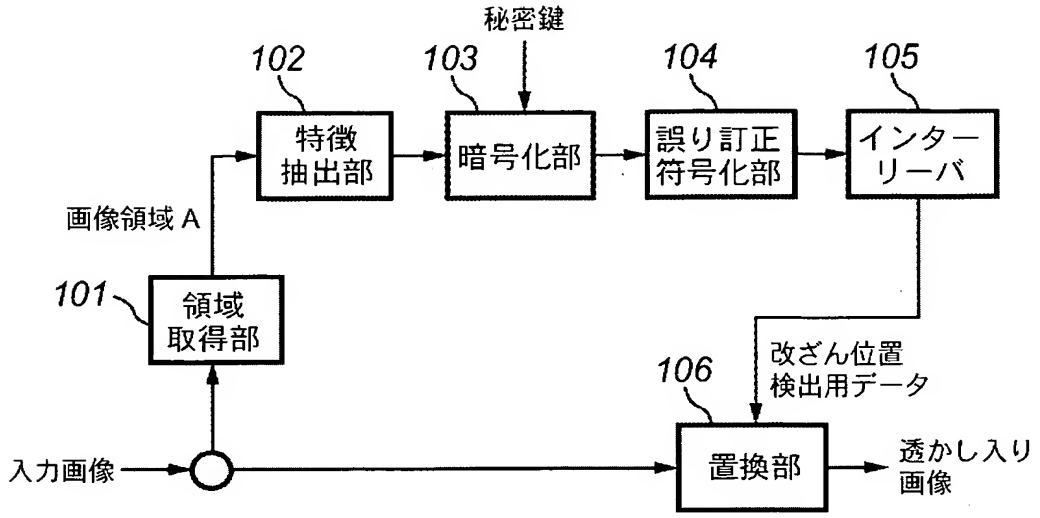
改ざんが行われた改ざん画像から改ざん位置を判定する処理を説明するための図である。

【図２３】

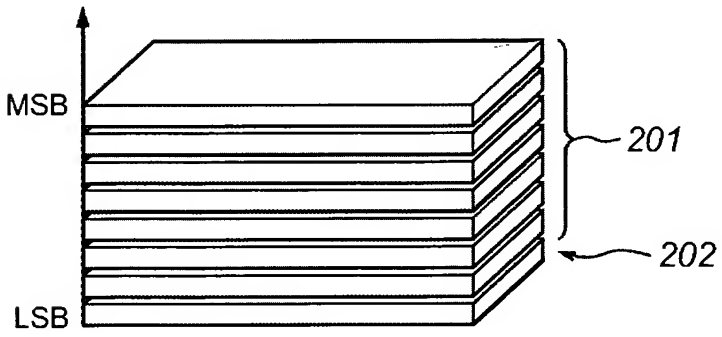
第２改ざん位置特定ビット系列Ｓ（ＢＳ）と改ざん画像との対応を示す図である。

【書類名】　図面

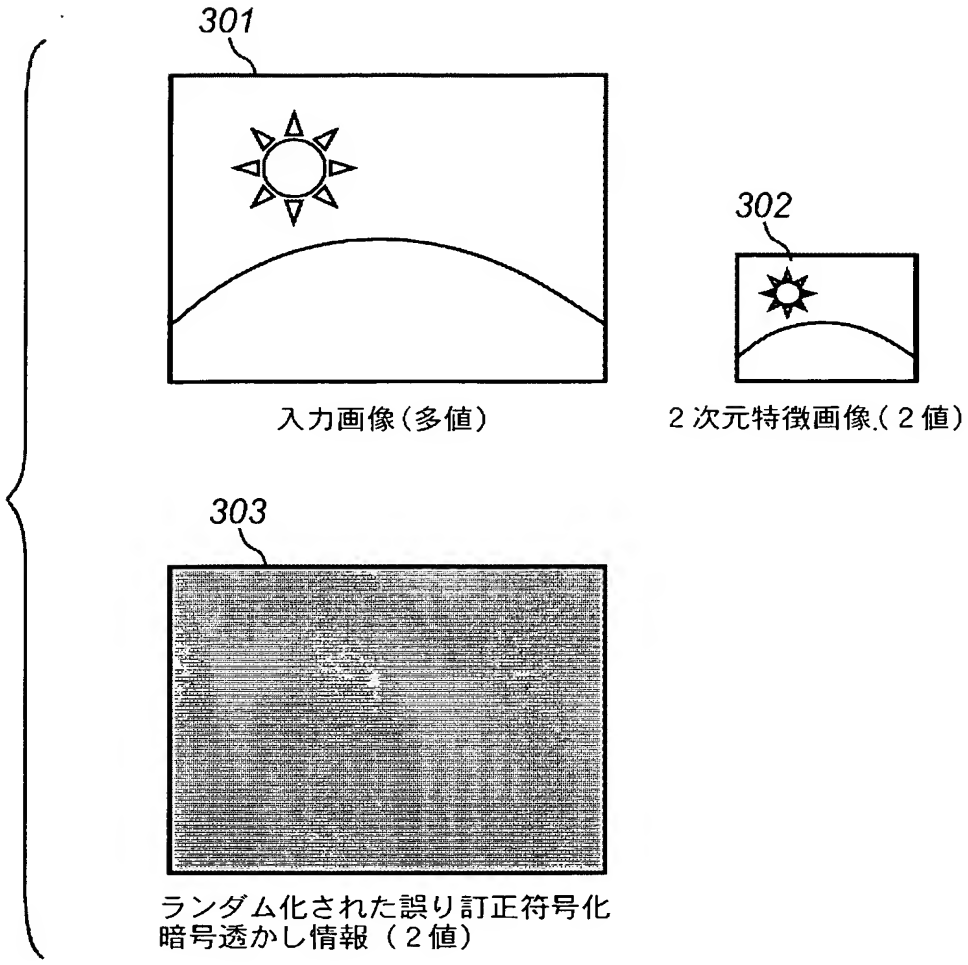
【図１】


秘密鍵
102
103
104
105
特徴
抽出部
暗号化部
誤り訂正
符号化部
インター
リーバ
画像領域Ａ
101
領域
取得部
106
改ざん位置
検出用データ
入力画像
置換部
透かし入り
画像

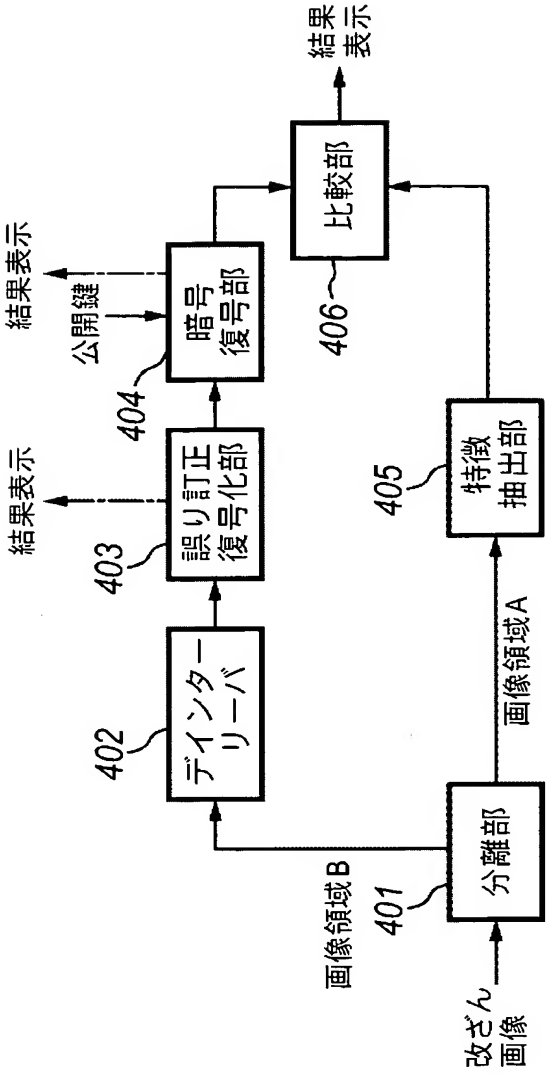
【図２】


MSB
LSB
201
202

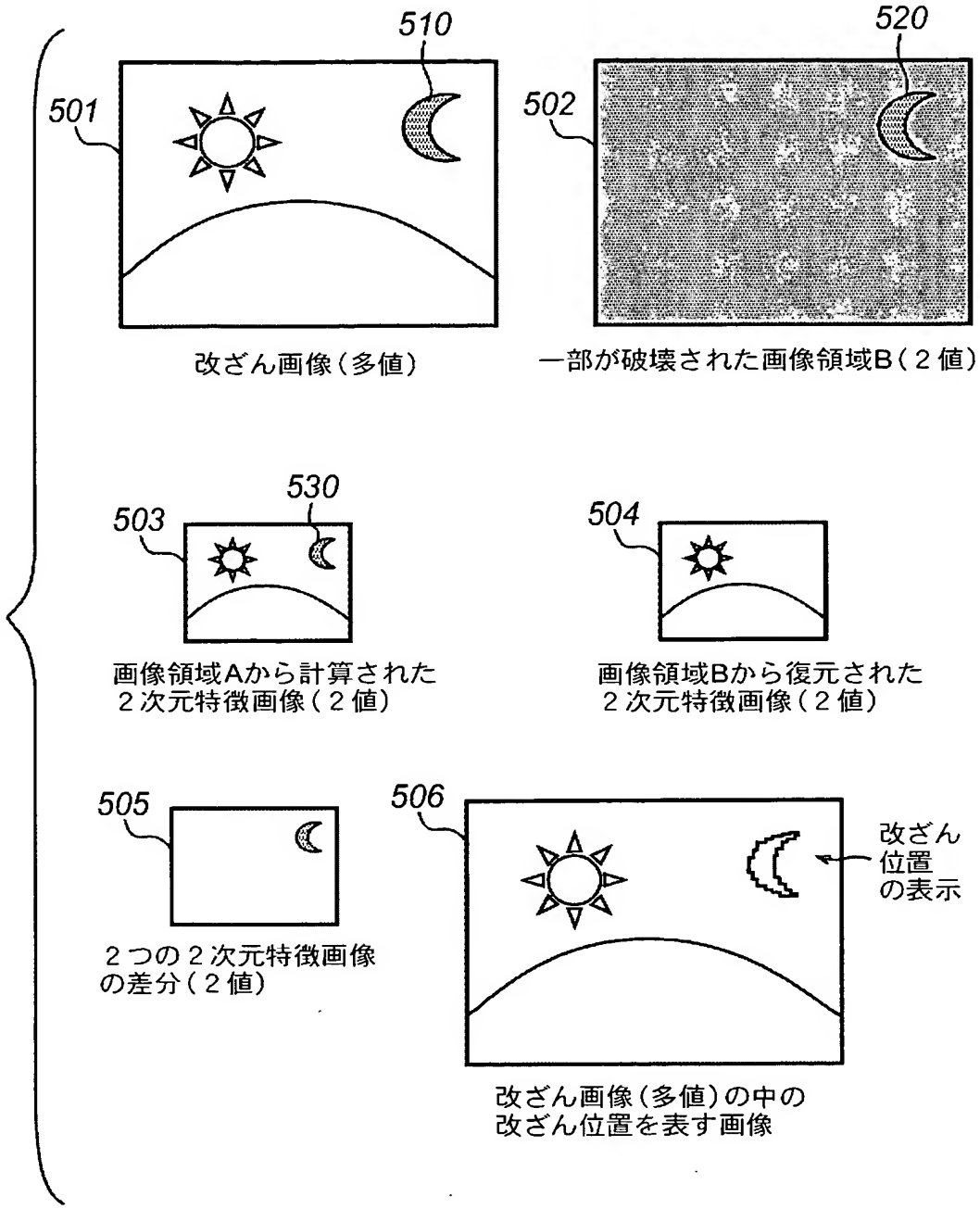
【図３】



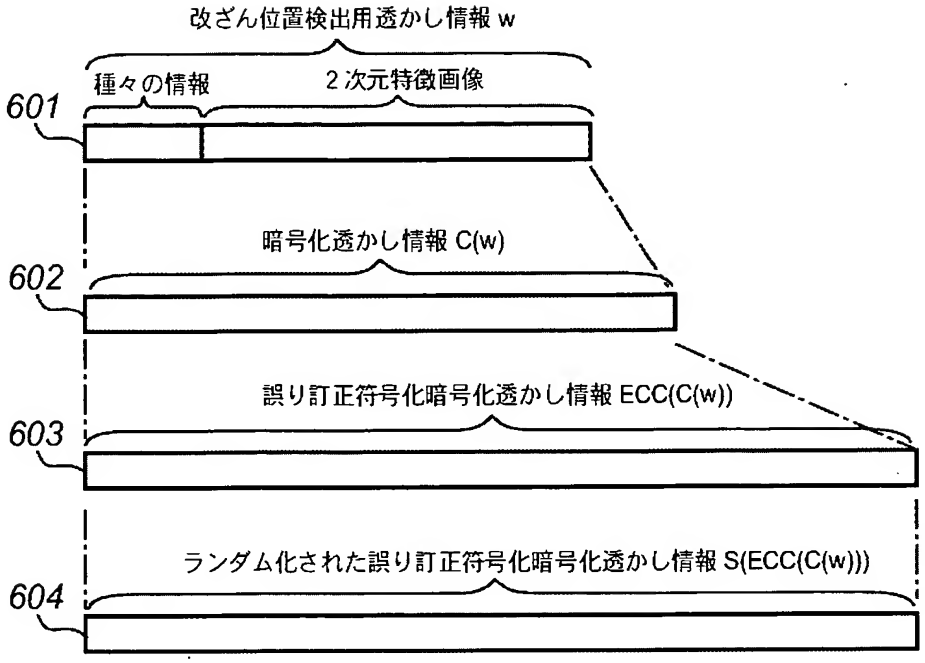
【図４】


結果表示
比較部
406
暗号復号部
404
公開鍵
結果表示
誤り訂正復号化部
403
結果表示
デインターリーバ
402
画像領域B
分離部
401
画像領域A
特徴抽出部
405
改ざん画像

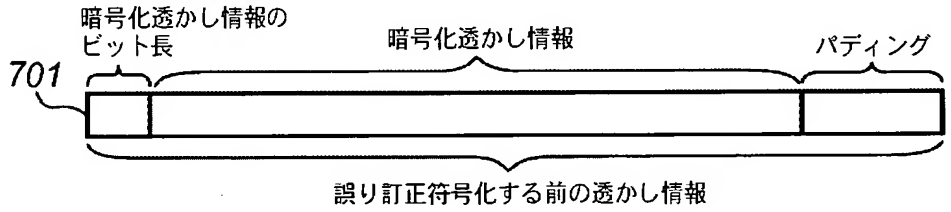
【図５】


510
501
520
502
改ざん画像（多値）
一部が破壊された画像領域B（２値）
530
503
504
画像領域Aから計算された
２次元特徴画像（２値）
画像領域Bから復元された
２次元特徴画像（２値）
505
506
改ざん
位置
の表示
２つの２次元特徴画像
の差分（２値）
改ざん画像（多値）の中の
改ざん位置を表す画像

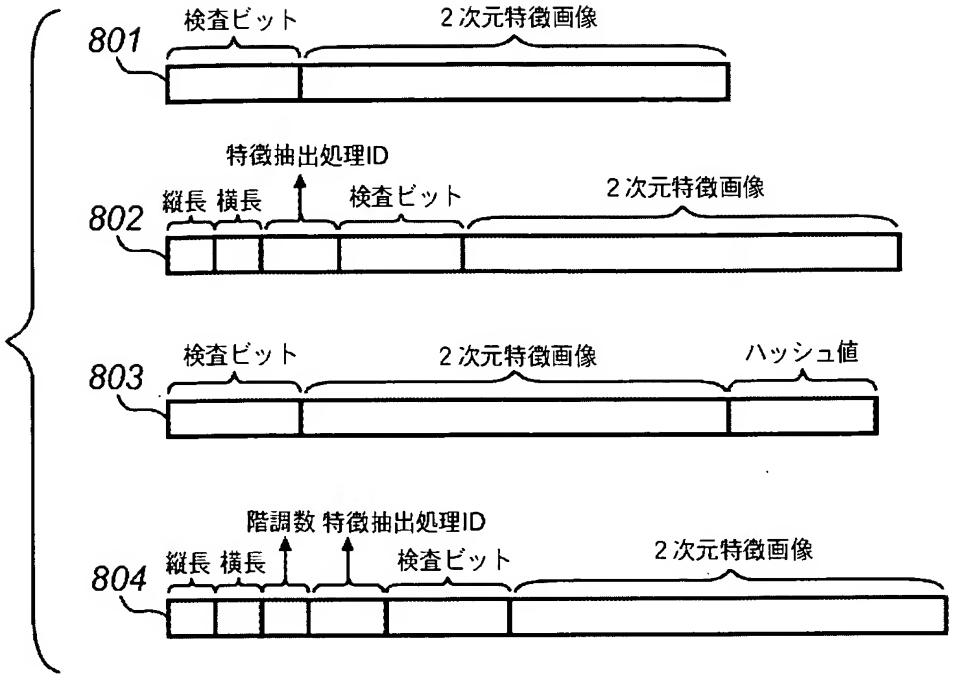
【図６】


改ざん位置検出用透かし情報 w
種々の情報
２次元特徴画像
601
暗号化透かし情報 C(w)
602
誤り訂正符号化暗号化透かし情報 ECC(C(w))
603
ランダム化された誤り訂正符号化暗号化透かし情報 S(ECC(C(w)))
604

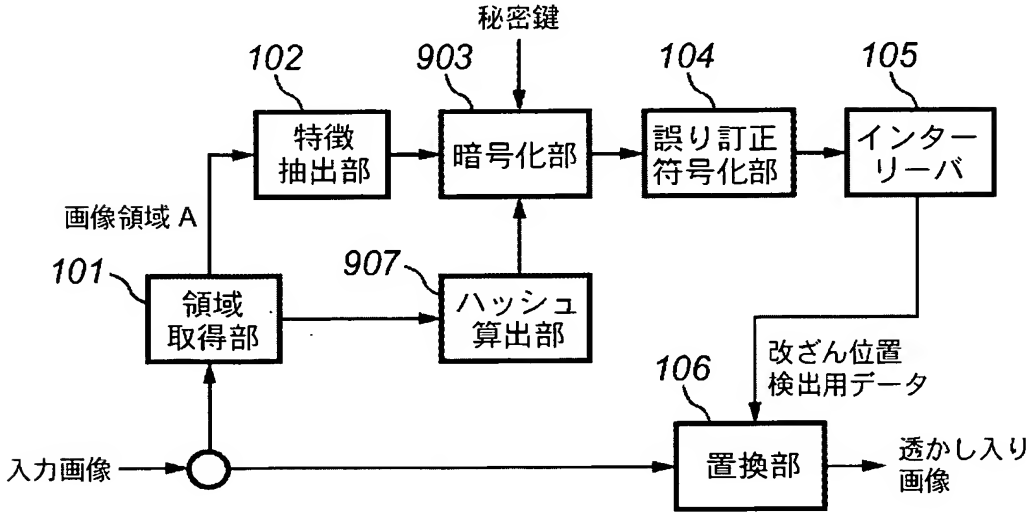
【図７】


暗号化透かし情報の
ビット長
暗号化透かし情報
パディング
701
誤り訂正符号化する前の透かし情報

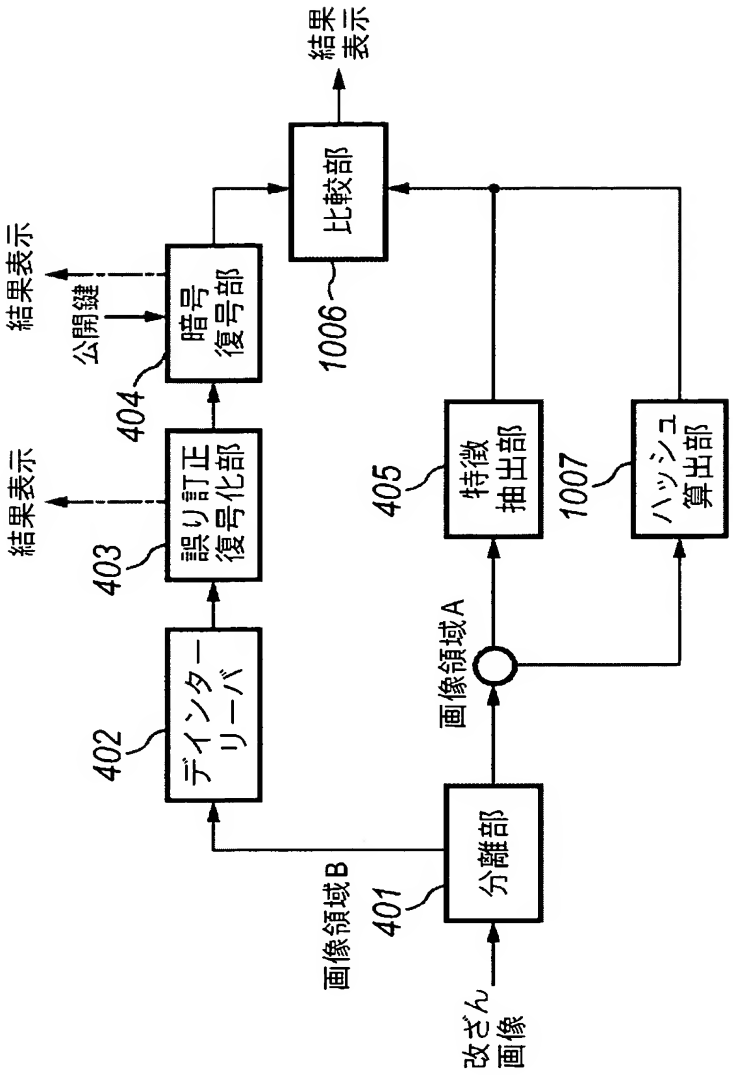
【図８】


801
検査ビット
２次元特徴画像
802
特徴抽出処理ID
縦長 横長
検査ビット
２次元特徴画像
803
検査ビット
２次元特徴画像
ハッシュ値
804
階調数 特徴抽出処理ID
縦長 横長
検査ビット
２次元特徴画像

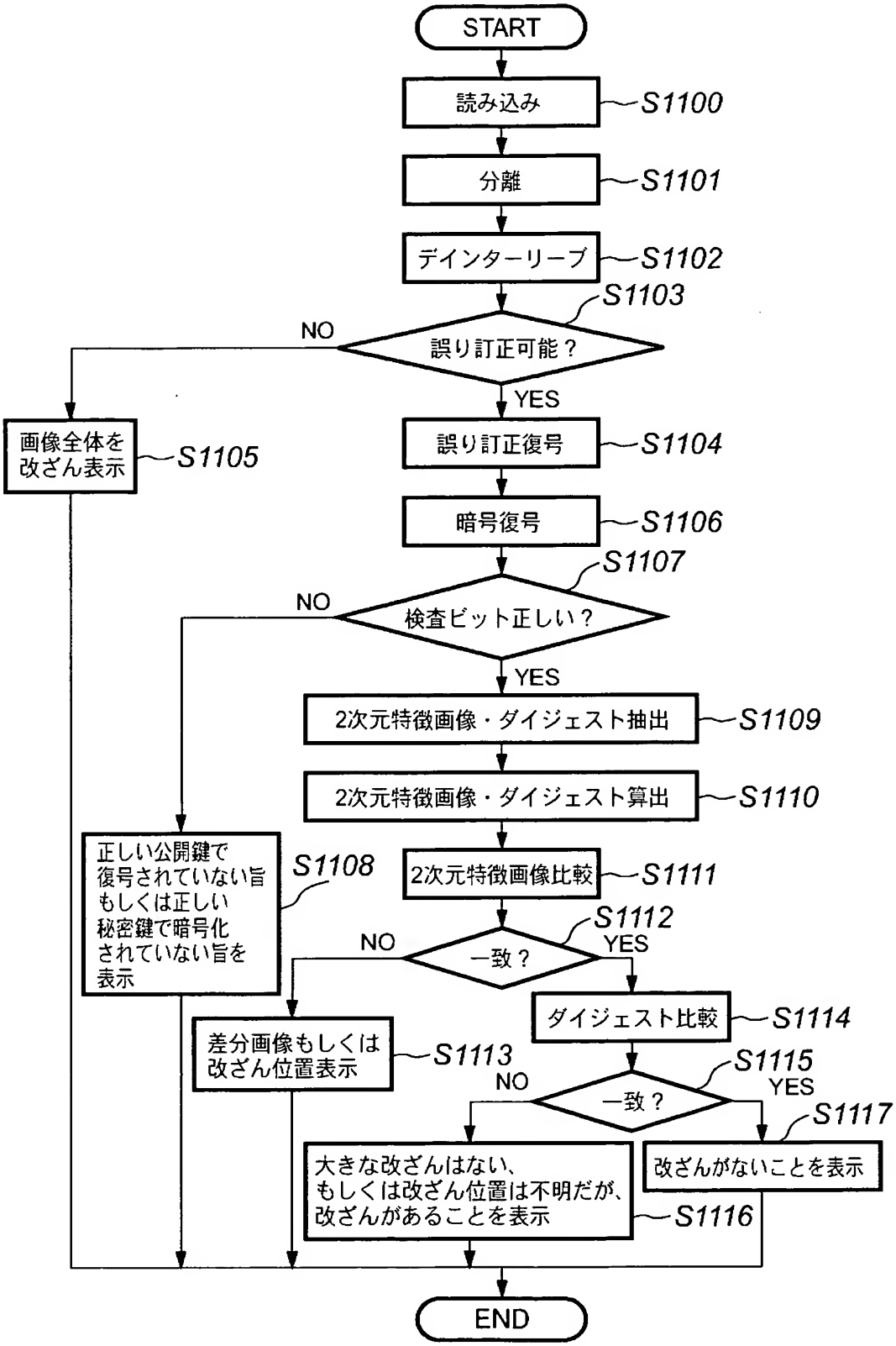
【図９】


秘密鍵
102
903
104
105
特徴
抽出部
暗号化部
誤り訂正
符号化部
インター
リーバ
画像領域 A
101
907
領域
取得部
ハッシュ
算出部
106
改ざん位置
検出用データ
入力画像
置換部
透かし入り
画像

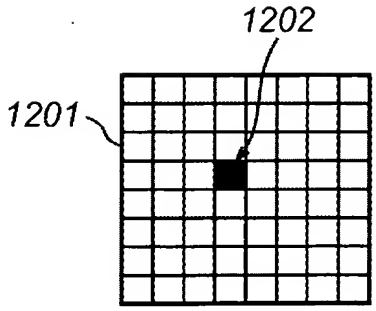
【図１０】


結果表示
比較部
1006
結果表示
公開鍵
暗号復号部
404
結果表示
誤り訂正復号化部
403
デインターリーバ
402
画像領域B
分離部
401
改ざん画像
画像領域A
特徴抽出部
405
ハッシュ算出部
1007

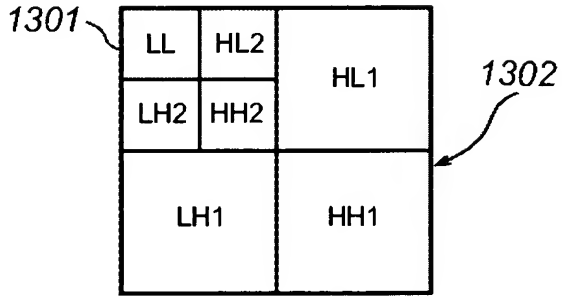
【図１１】


START
読み込み
S1100
分離
S1101
デインターリーブ
S1102
S1103
誤り訂正可能？
NO
YES
画像全体を改ざん表示
S1105
誤り訂正復号
S1104
暗号復号
S1106
S1107
検査ビット正しい？
NO
YES
2次元特徴画像・ダイジェスト抽出
S1109
2次元特徴画像・ダイジェスト算出
S1110
正しい公開鍵で復号されていない旨もしくは正しい秘密鍵で暗号化されていない旨を表示
S1108
2次元特徴画像比較
S1111
S1112
一致？
NO
YES
差分画像もしくは改ざん位置表示
S1113
ダイジェスト比較
S1114
S1115
一致？
NO
YES
S1117
大きな改ざんはない、もしくは改ざん位置は不明だが、改ざんがあることを表示
S1116
改ざんがないことを表示
END

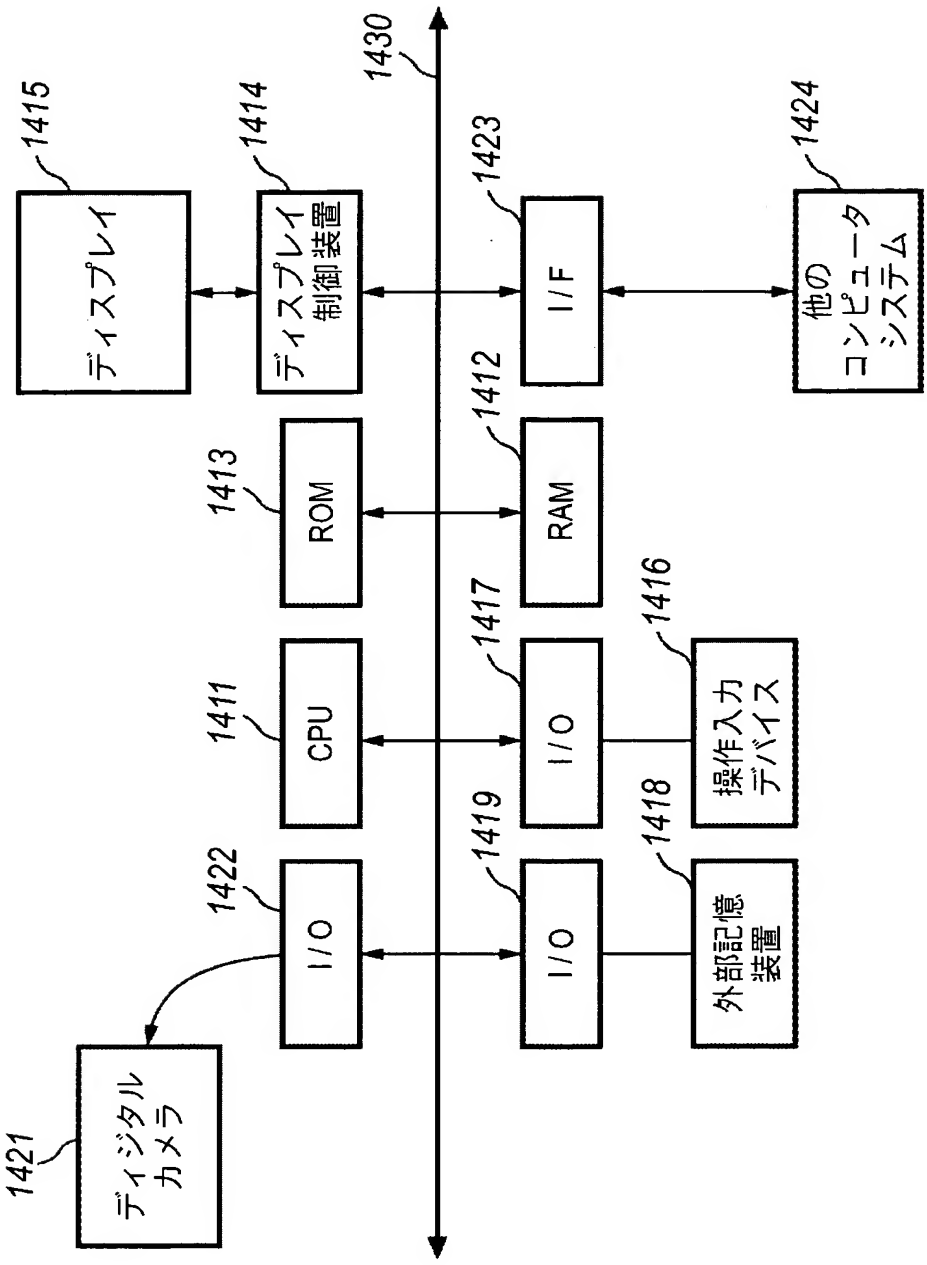
【図１２】



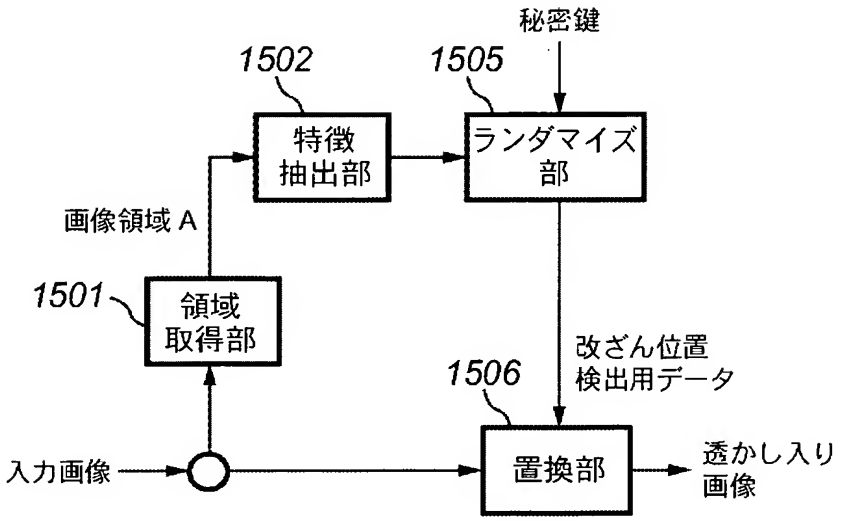
【図１３】



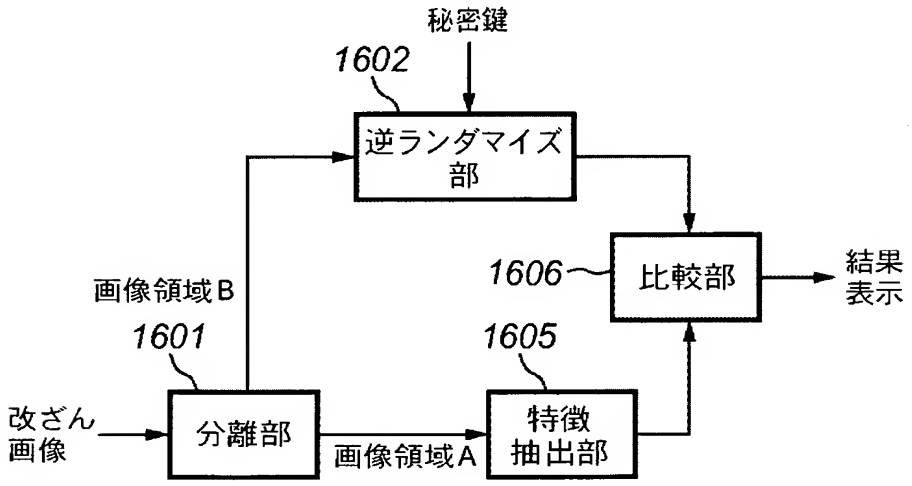
【図１４】


1430
1415
ディスプレイ
1414
ディスプレイ制御装置
1423
I/F
1424
他のコンピュータシステム
1412
1413
ROM
RAM
1417
1416
1411
CPU
I/O
操作入力デバイス
1419
1418
1422
I/O
I/O
外部記憶装置
1421
ディジタルカメラ

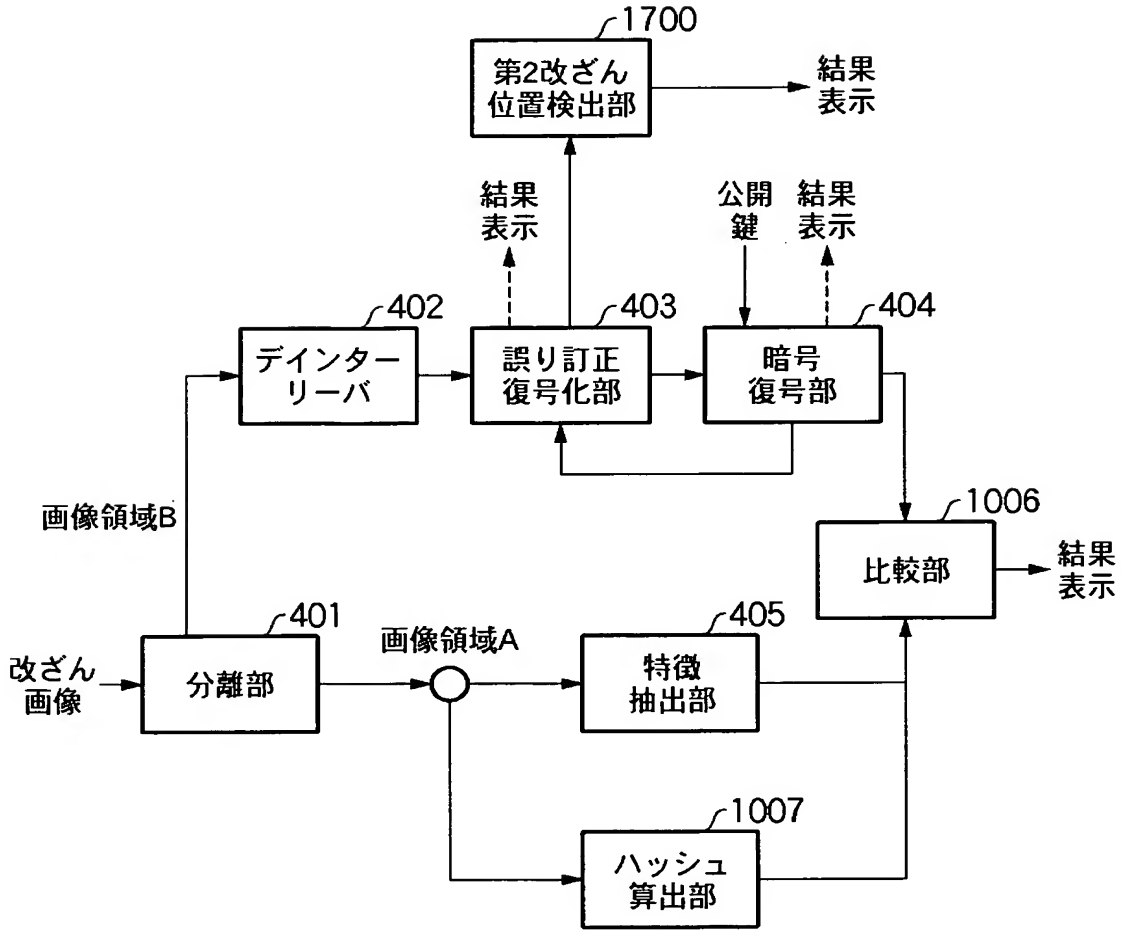
【図１５】


秘密鍵
1502
1505
特徴
抽出部
ランダマイズ
部
画像領域Ａ
1501
領域
取得部
改ざん位置
検出用データ
1506
入力画像
置換部
透かし入り
画像

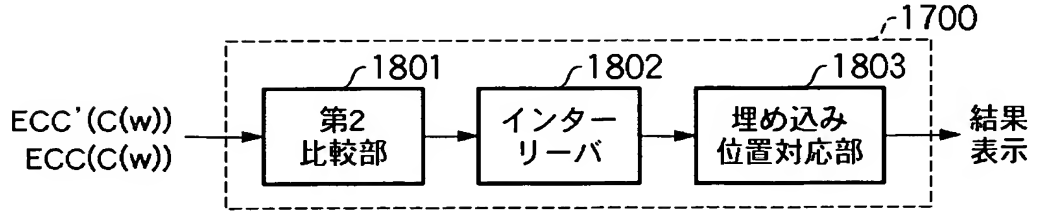
【図１６】


秘密鍵
1602
逆ランダマイズ
部
1606
比較部
結果
表示
画像領域Ｂ
1601
1605
改ざん
画像
分離部
画像領域Ａ
特徴
抽出部

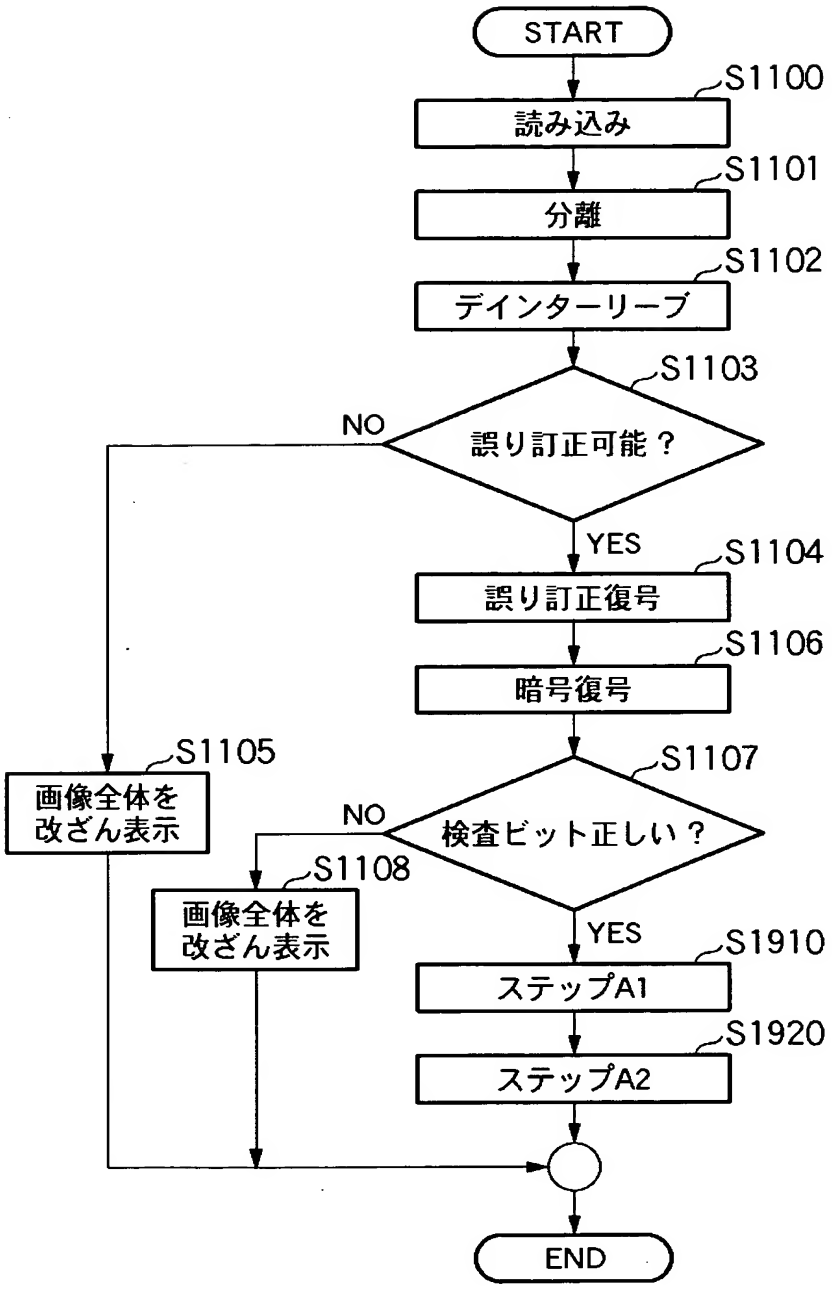
【図１７】


1700
第2改ざん
位置検出部
結果
表示
結果
表示
公開
鍵
結果
表示
402
403
404
デインター
リーバ
誤り訂正
復号化部
暗号
復号部
画像領域B
1006
比較部
結果
表示
401
画像領域A
405
改ざん
画像
分離部
特徴
抽出部
1007
ハッシュ
算出部

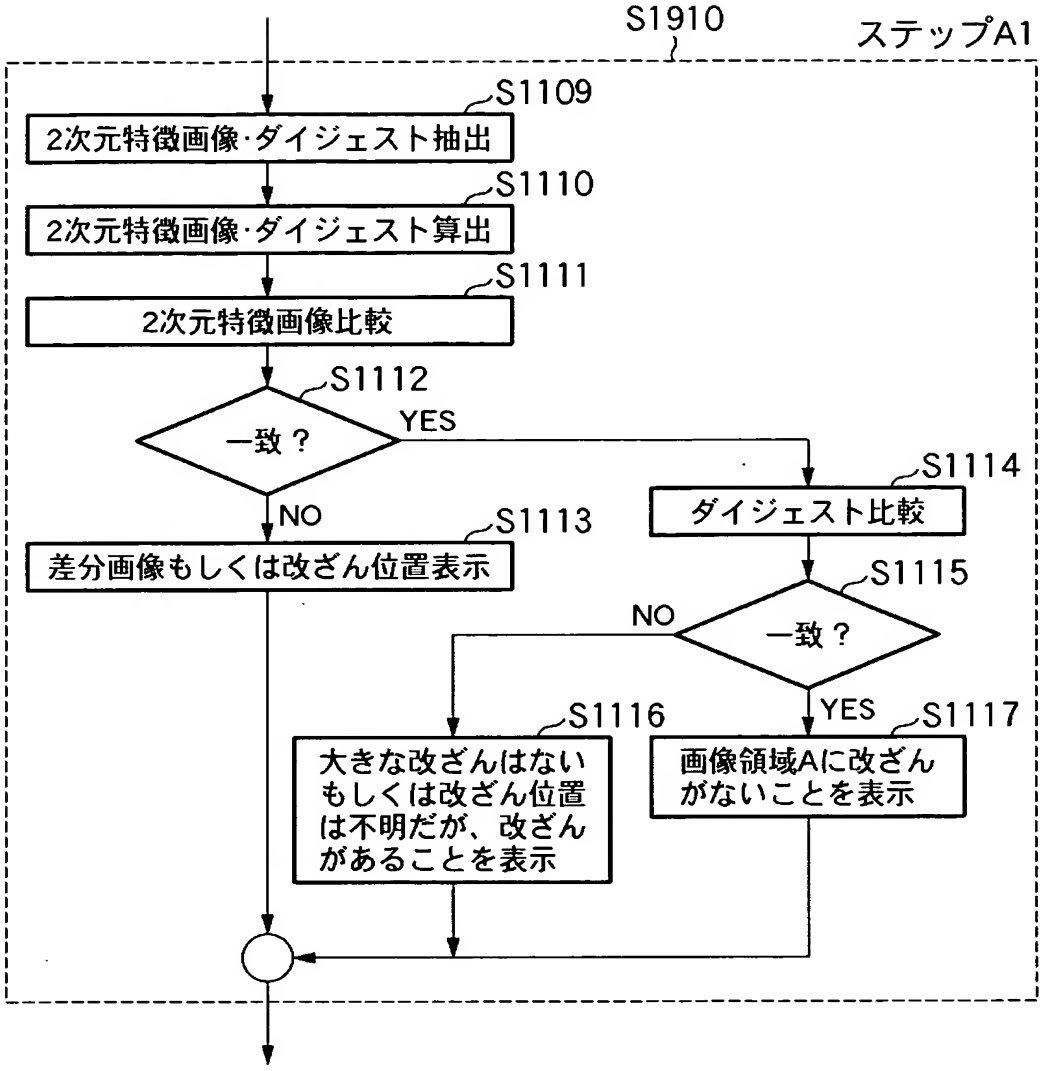
【図１８】


1700
1801
1802
1803
ECC'(C(w))
ECC(C(w))
第2
比較部
インター
リーバ
埋め込み
位置対応部
結果
表示

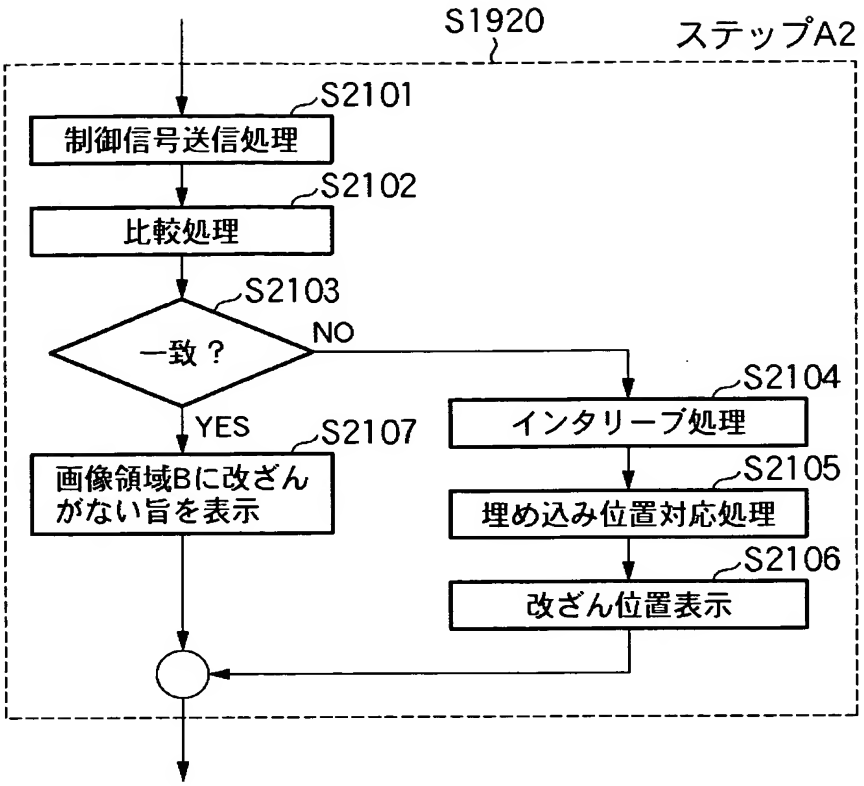
【図１９】


START
S1100
読み込み
S1101
分離
S1102
デインターリーブ
S1103
誤り訂正可能？
NO
YES
S1104
誤り訂正復号
S1106
暗号復号
S1107
検査ビット正しい？
NO
YES
S1105
画像全体を
改ざん表示
S1108
画像全体を
改ざん表示
S1910
ステップA1
S1920
ステップA2
END

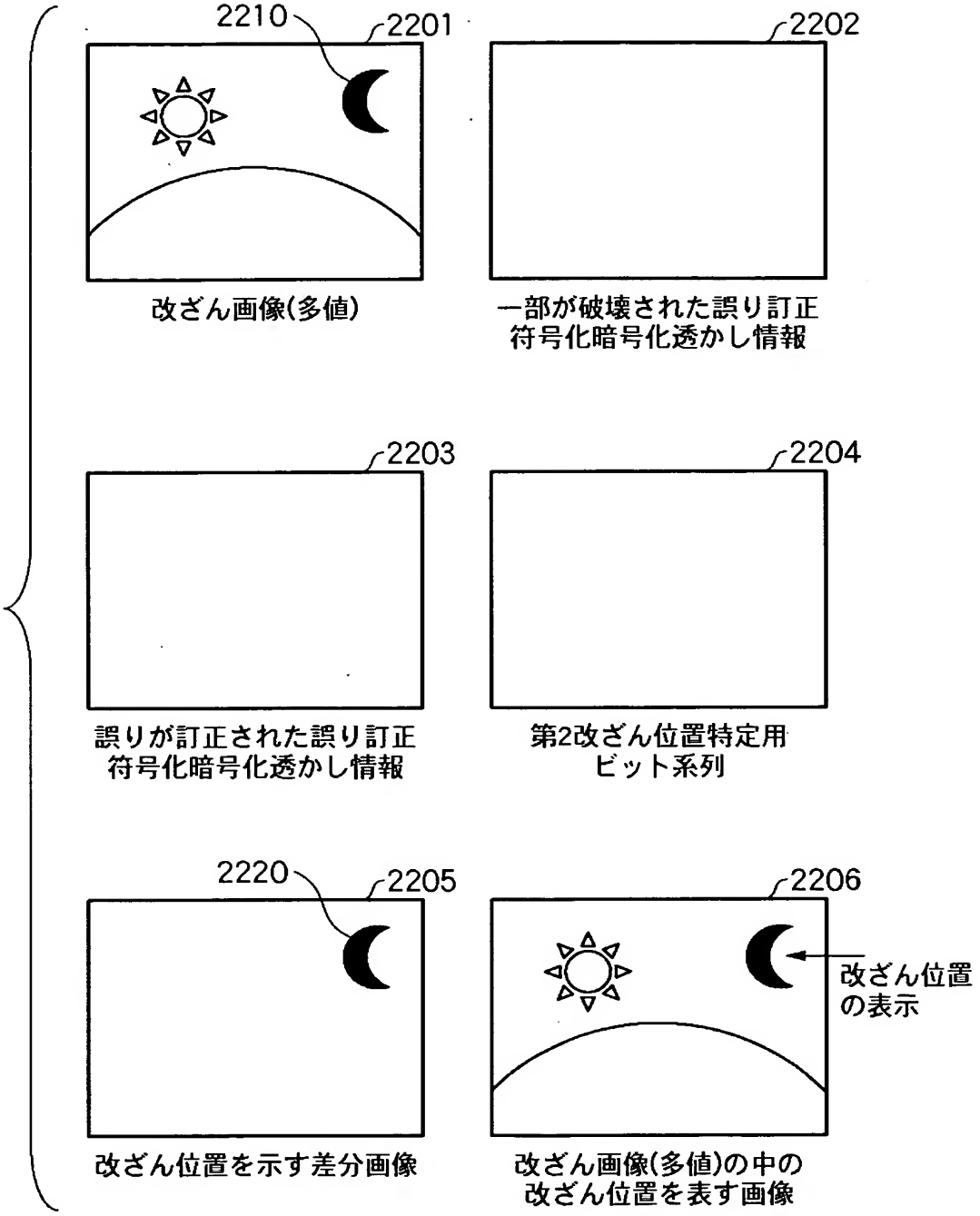
【図２０】


S1910
ステップA1
S1109
2次元特徴画像･ダイジェスト抽出
S1110
2次元特徴画像･ダイジェスト算出
S1111
2次元特徴画像比較
S1112
一致？
YES
NO
S1113
差分画像もしくは改ざん位置表示
S1114
ダイジェスト比較
S1115
一致？
NO
YES
S1116
大きな改ざんはないもしくは改ざん位置は不明だが、改ざんがあることを表示
S1117
画像領域Aに改ざんがないことを表示

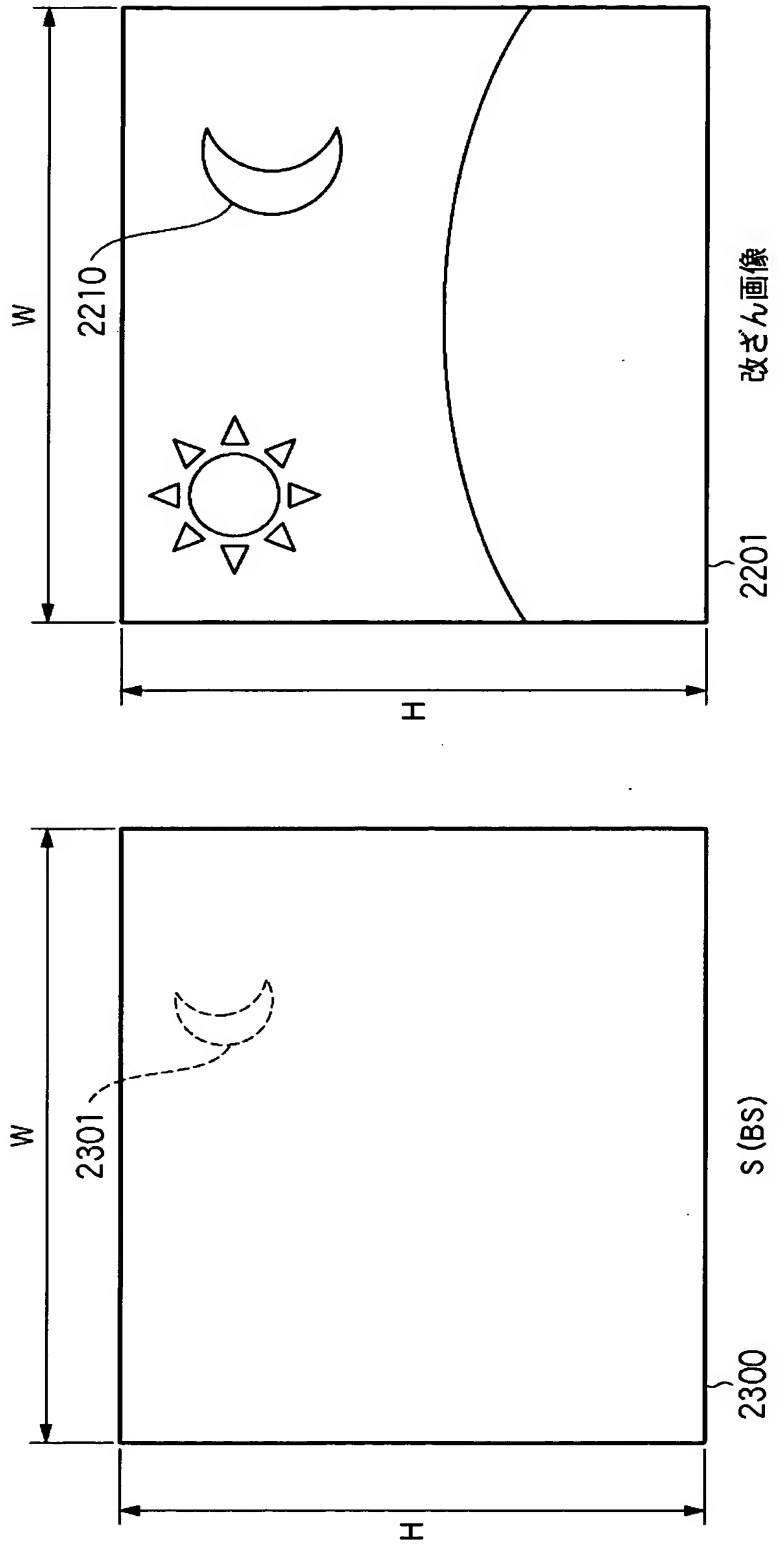
【図２１】


S1920
ステップA2
S2101
制御信号送信処理
S2102
比較処理
S2103
一致？
NO
YES
S2104
インタリーブ処理
S2105
埋め込み位置対応処理
S2106
改ざん位置表示
S2107
画像領域Bに改ざんがない旨を表示

【図２２】


2210
2201
改ざん画像(多値)
2202
一部が破壊された誤り訂正
符号化暗号化透かし情報
2203
誤りが訂正された誤り訂正
符号化暗号化透かし情報
2204
第2改ざん位置特定用
ビット系列
2220
2205
改ざん位置を示す差分画像
2206
改ざん位置
の表示
改ざん画像(多値)の中の
改ざん位置を表す画像

【図２３】



【書類名】　要約書

【要約】

【課題】　画像に対する改竄の位置を正確に検出すること。

【解決手段】　特徴抽出部１０２は、第１の領域と第２の領域とで構成される原画像中の第１の領域の画像を用いて、原画像の特徴画像を生成し、暗号化部１０３は特徴画像と原画像に関する情報とを含む透かし情報を生成する。そして誤り訂正符号化部１０４は、透かし情報に対して誤り訂正符号化を行い、誤り訂正符号化透かし情報を生成し、置換部１０６は原画像において、第２の領域の画像情報を誤り訂正符号化透かし情報に置き換えた画像を出力画像として出力する。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２００３－１０５４９８
受付番号	５０３００５８９２４０
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１５年　４月１４日

＜認定情報・付加情報＞

【特許出願人】
- 【識別番号】　000001007
- 【住所又は居所】　東京都大田区下丸子３丁目３０番２号
- 【氏名又は名称】　キヤノン株式会社

【代理人】　申請人
- 【識別番号】　100076428
- 【住所又は居所】　東京都千代田区紀尾井町３番６号　秀和紀尾井町パークビル７Ｆ　大塚国際特許事務所
- 【氏名又は名称】　大塚　康徳

【選任した代理人】
- 【識別番号】　100112508
- 【住所又は居所】　東京都千代田区紀尾井町３番６号　秀和紀尾井町パークビル７Ｆ　大塚国際特許事務所
- 【氏名又は名称】　高柳　司郎

【選任した代理人】
- 【識別番号】　100115071
- 【住所又は居所】　東京都千代田区紀尾井町３番６号　秀和紀尾井町パークビル７Ｆ　大塚国際特許事務所
- 【氏名又は名称】　大塚　康弘

【選任した代理人】
- 【識別番号】　100116894
- 【住所又は居所】　東京都千代田区紀尾井町３番６号　秀和紀尾井町パークビル７Ｆ　大塚国際特許事務所
- 【氏名又は名称】　木村　秀二

次頁無

特願２００３－１０５４９８

出　願　人　履　歴　情　報

識別番号　［０００００１００７］

１．変更年月日　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都大田区下丸子３丁目３０番２号
氏　名　キヤノン株式会社